PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-261550

(43)Date of publication of application : 24.09.1999

(51)Int.Cl. H04L 9/32
G06F 12/14
G06F 17/21
G09C 1/00

(21)Application number : 10-271541

(22)Date of filing : 25.09.1998

(71)Applicant : TOSHIBA CORP

(72)Inventor : ONO KAZUTERU

(30)Priority

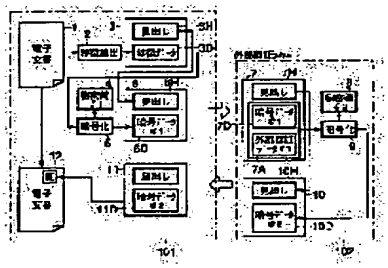
Priority number : 10 717 Priority date : 06.01.1998 Priority country : JP

(54) SYSTEM AND METHOD FOR PREVENTING ELECTRONIC DOCUMENT FORGERY

(57)Abstract:

PROBLEM TO BE SOLVED: To add an evidence capability to an electronic document and also to promote document computerization in a true sense.

SOLUTION: This system is provided with a characteristics extracting means 11 which extracts a characteristics and produces characteristics data, a 1st enciphering means 5 which enciphers the characteristics data with the 1st key of cryptograph of the 1st person concerned and produces 1st enciphered data, a 2nd enciphering means 9 which adds external authentication data including at least a date to the 1st enciphered data enciphers it with the 2nd key of cryptograph of an external authenticating person and produces 2nd enciphered data, and a means which authenticates the 2nd enciphered data as authentication data of the electronic document.



LEGAL STATUS

[Date of request for examination] 05.03.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] A feature-extraction means to extract the description from an electronic filing document and to generate the description data, The 1st encryption means which enciphers said description data by the 1st cryptographic key, and generates the 1st encryption data, The alteration prevention system of an electronic filing document equipped with the 2nd encryption means which adds external authentication data to said 1st encryption data, enciphers this by the 2nd cryptographic key, and generates the 2nd encryption data, and the means which uses said 2nd encryption data as the authentication data of said electronic filing document.
[Claim 2] A feature-extraction means to extract the description from an electronic filing document and to generate the description data, the 1st encryption means which enciphers said description data by the 1st cryptographic key, and generates the 1st encryption data, The document authentication system equipped with the 1st means of communications which receives authentication data, and a means to make said authentication data correspond to said electronic filing document while transmitting said 1st encryption data, The external authentication data which contain the date in said 1st encryption data transmitted in said 1st means of communications at least are added. The 2nd encryption means which enciphers this by the 2nd cryptographic key and generates the 2nd encryption data, And the alteration prevention system of the electronic filing document equipped with the external authentication system equipped with the 2nd means of communications which transmits to said document authentication system by using said 2nd encryption data as authentication data while receiving said 1st encryption data.
[Claim 3] It is the alteration prevention system of the electronic filing document according to claim 1 or 2 characterized by having the 3rd encryption means which enciphers said 1st encryption data by the 3rd cryptographic key, and generates the 3rd encryption data, replacing said 2nd encryption means with said 1st encryption data, adding external authentication data to said 3rd encryption data, enciphering by the 2nd cryptographic key, and generating the 2nd encryption data.
[Claim 4] The alteration prevention system of the electronic filing document according to claim 1, 2, or 3 characterized by having the 4th encryption ****** which enciphers said 2nd encryption data by the 4th different cryptographic key from said 2nd cryptographic key, generates the 4th encryption data, and is used as said authentication data.
[Claim 5] The 2nd decryption means which picks out the 2nd encryption data from the authentication data corresponding to the electronic filing document for authentication, and decrypts this with the 2nd public key corresponding to the 2nd cryptographic key, The 1st decryption means which picks out the 1st encryption data from the data decrypted by said 2nd decryption means, and decrypts this with the 1st public key corresponding to the 1st cryptographic key, The authentication-text document check system characterized by having a feature-extraction means to extract the description from said electronic filing document, and to generate the description data for enquiry, and a collating means to pick out the description data from the data decrypted by said 1st decryption means, and to collate with said description data for enquiry.
[Claim 6] In claim 5, the 3rd encryption data is picked out from the data decrypted by said 2nd decryption means. The 3rd decryption means which decrypts this with the 3rd public key corresponding

to the 3rd cryptographic key is established. Said 1st decryption means is an authentication-text document check system characterized by picking out the 1st encryption data from the data decrypted by said 3rd decryption means, and decrypting this with the 1st public key corresponding to the 1st cryptographic key.

[Claim 7] reading appearance of the one every unit of the data for a feature extraction being carried out, and with the 1st train generation means which puts the total value which comes to add only the number of unit of a convention of the read value in order in order one by one, and is made into the 1st total value train The value used as the relation which separated only the number of unit of said convention to this value that it read at a time one unit which it read at a time one unit is added. The 2nd train generation means which adds the value which serves as said relation to this added value, and which it read at a time one unit, repeats this addition, puts in order the total value acquired by adding the number-of-unit time of said convention as a count of adding one by one, and is made into the 2nd total value train, Feature-extraction equipment characterized by having a means to output said 1st total value train and said 2nd total value train as description data.

[Claim 8] reading appearance of the one every unit of said 1st total value train being carried out, and with the 3rd train generation means which puts the total value which comes to add only the number of unit of a convention of the read value in order in order one by one, and is made into the 3rd total value train reading appearance of the one every unit of said 2nd total value train being carried out, and with the 4th train generation means which puts the total value which comes to add only the number of unit of a convention of the read value in order in order one by one, and is made into the 4th total value train Feature-extraction equipment according to claim 7 characterized by having a means to output said 3rd total value train and said 4th total value train as description data.

[Claim 9] A fingerprint reading means and a fingerprint feature-extraction means to perform a feature extraction from the fingerprint data read with said fingerprint reading means, and to generate the fingerprint description data, A cryptographic key generation means to generate a cryptographic key from said fingerprint description data and a password, A private key public key generation means to generate a private key and a public key from said fingerprint description data, a password, and a random-number value, the data, the fingerprint data, and the password which were enciphered with an encryption means to encipher said cryptographic key itself and said private key by said cryptographic key, respectively, and said encryption means -- him -- him who is characterized by having the means used as authentication data -- an authentication data generative system.

[Claim 10] him who was indicated by said claim 9 -- said him who generated with the authentication data generative system -- with the password in authentication data When both passwords are in agreement with a password collating means to collate the entered password, and a fingerprint reading means said fingerprint reading means -- fingerprint reading -- carrying out -- said him -- with the fingerprint data in authentication data When fingerprint authentication is in agreement with a fingerprint authentication means to collate the fingerprint data read with said fingerprint reading means said him -- with a fingerprint feature-extraction means to perform a feature extraction from the fingerprint data in authentication data, and to generate the fingerprint description data A cryptographic key generation means to generate a cryptographic key from the fingerprint description data generated with said fingerprint feature-extraction means, and a password, The cryptographic key as which it was enciphered in authentication data is decoded. this generated cryptographic key -- him -- the case where cryptographic key collating is in agreement with a cryptographic key collating means to collate said generated cryptographic key and the decoded cryptographic key -- this cryptographic key -- using -- said him -- the private key decode system equipped with a private key decode means to decode the private key enciphered in authentication data.

[Claim 11] Fingerprint data extraction equipment characterized by to have a fingerprint reading means, a boundary detection means detect the boundary of the fingerprint data read in said fingerprint reading means, the embossing means that carries out embossing processing of the fingerprint data by which

boundary detection was carried out with said boundary detection means, and the profile trace means which carries out profile trace of the fingerprint data by which embossing processing was carried out with said embossing means.

[Claim 12] The field fetch means which takes out two or more rectangle fields from the fingerprint data extracted from the fingerprint data extraction equipment indicated by said claim 11, A pattern-matching means to judge whether the data of said rectangle field are compared with two or more patterns registered beforehand, and it matches with which pattern, Fingerprint feature-extraction equipment characterized by having the means which puts the numeric value corresponding to the matched pattern in order as a sequence of numbers, and uses the sequence of numbers concerned as the fingerprint description data.

[Claim 13] The feature-extraction step which extracts the description from an electronic filing document and generates the description data, The 1st encryption step which enciphers said description data by the 1st cryptographic key of the 1st person concerned, and generates the 1st encryption data, The 2nd encryption step which adds the external authentication data which contain the date in said 1st encryption data at least, enciphers this by an external authentication person's 2nd cryptographic key, and generates the 2nd encryption data, The alteration prevention approach of the electronic filing document characterized by having the step which uses said 2nd encryption data as the authentication data of said electronic filing document.

[Claim 14] The document authentication system which enciphers the data extracted from the electronic filing document by the 1st cryptographic key, and generates the 1st encryption data, The external authentication system which enciphers received data by the 2nd cryptographic key, and generates the 2nd encryption data is an alteration prevention system of an electronic filing document connected by the communication line. Said 1st encryption data generated in the document authentication system is transmitted to said external authentication system through said communication line. In an external authentication system The external authentication data which contain the date in said 1st received encryption data at least are added. This is enciphered by the 2nd cryptographic key, the 2nd encryption data is generated, and it transmits to said document authentication system by using this 2nd encryption data as authentication data. In a document authentication system The alteration prevention approach of the electronic filing document characterized by making it correspond to said electronic filing document, using said 2nd received encryption data as authentication data.

[Claim 15] In the 1st document authentication system, encipher the data extracted from the electronic filing document by the 1st cryptographic key, and the 1st encryption data is generated. Encipher said 1st encryption data which transmitted to the 2nd document authentication system and was transmitted from said 1st document authentication system in the 2nd document authentication system by the 3rd cryptographic key, and the 3rd encryption data is generated. External authentication data are added to said 3rd encryption data which transmitted to the external authentication system and was transmitted from said 2nd document authentication system in the external authentication system. Encipher this by the 2nd cryptographic key, generate the 2nd encryption data, and it transmits to said 1st document authentication system at least. The alteration prevention approach of the electronic filing document characterized by making it correspond to said electronic filing document in the 1st document authentication system concerned, using said 2nd received encryption data as authentication data.

[Claim 16] The 2nd decryption step corresponding to drawing for said 2nd encryption data decrypted with the 2nd public key corresponding to said 2nd private key for this from said authentication data generated by the alteration prevention system of said electronic filing document according to claim 1, 2, or 3, The 1st decryption step corresponding to drawing for said 1st encryption data decrypted from the data decrypted by said 2nd decryption step with the 1st public key corresponding to said 1st private key for this, The feature-extraction step which extracts the description from said electronic filing document, and generates the description data for collating, The collating step which collates said description data with drawing from the data decrypted by said 1st decryption step, and collates this with said description

data for collating, The authentication-text document symptom characterized by having the step which outputs the fact of authentication by the external authentication person, and the date of authentication with said external authentication data picked out from the data decrypted by the collating result by said collating step, and said 2nd decryption means.

[Claim 17] A feature-extraction means to extract the description from an electronic filing document and to generate the description data, The 1st encryption means which enciphers said description data by the 1st cryptographic key of the 1st person concerned, and generates the 1st encryption data, While the 2nd encryption data with which the external authentication data which contain the date at least are added, and an external authentication person's 2nd cryptographic key comes to encipher this is inputted into said 1st encryption data The record medium which recorded the program for operating a computer as a means which uses this 2nd encryption data as the authentication data of said electronic filing document and in which computer reading is possible.

[Claim 18] The 2nd decryption means corresponding to drawing for said 2nd encryption data decrypted with the 2nd public key corresponding to said 2nd private key for this from said authentication data generated by the alteration prevention system of said electronic filing document according to claim 1, 2, or 3, The 1st decryption means corresponding to drawing for said 1st encryption data decrypted from the data decrypted by said 2nd decryption means with the 1st public key corresponding to said 1st private key for this, A feature-extraction means to extract the description from said electronic filing document, and to generate the description data for collating, A collating means to collate said description data with drawing from the data decrypted by said 1st decryption means, and to collate this with said description data for collating, With said external authentication data picked out from the data decrypted by the collating result by said collating means, and said 2nd decryption means The record medium which recorded the program for operating a computer as a means to output the fact of authentication by the external authentication person, and the date of authentication and in which computer reading is possible.

[Claim 19] The description is extracted from an electronic filing document, and the description data are generated, next said description data are enciphered by the 1st cryptographic key of the 1st person concerned. The 1st encryption data is generated. To next, said 1st encryption data The record medium with which the external authentication data which contain the date at least were added, this enciphered by an external authentication person's 2nd cryptographic key, the 2nd encryption data was generated, and the data which have the structure which finally consists of said 2nd encryption data were recorded and in which computer reading is possible.

[Claim 20] The description is extracted from an electronic filing document, and the description data are generated, next said description data are enciphered by the 1st cryptographic key of the 1st person concerned. The 1st encryption data is generated, next said 1st encryption data is enciphered by the 3rd cryptographic key of the 2nd person concerned. The 3rd encryption data is generated. To next, said 3rd encryption data The record medium with which the external authentication data which contain the date at least were added, this enciphered by an external authentication person's 2nd cryptographic key, the 2nd encryption data was generated, and the data which have the structure which finally consists of said 2nd encryption data were recorded and in which computer reading is possible.

[Claim 21] An electronic filing document is taken out from an electronic filing document with authentication. To this modification In addition, a document modification means to generate a new electronic filing document, the difference which extracts the changed part of the electronic filing document of the origin taken out from said electronic filing document with authentication, and said new electronic filing document, and acquires modification part data -- with an extract means While sending out each data attested by the modification person authentication means which carries out modification person authentication of said modification part data and said new electronic filing document, respectively, and said modification person authentication means to an external authentication system The alteration prevention system of the electronic filing document which receives the authentication

data by which external authentication was carried out in each, and is characterized by having modification part data with authentication, and an authentication means to generate a new electronic filing document with authentication, based on each received authentication data and said new electronic filing document.

[Claim 22] said modification person authentication means -- said modification part data -- and -- or the alteration prevention system of the electronic filing document according to claim 21 characterized by having a feature-extraction means to carry out a feature extraction from said new electronic filing document, and to output the description data, and an encryption means to encipher and output said description data with the encryption key of the modification person who generated said new electronic filing document.

[Claim 23] Said modification person authentication means is the alteration prevention system of the electronic filing document according to claim 22 characterized by having the coupling means which is outputted from said encryption means, and combines and outputs the encryption description data corresponding to said new electronic filing document, and authentication data before taking out from the original electronic filing document with authentication.

[Claim 24] Said modification person authentication means is the alteration prevention system of the electronic filing document according to claim 22 characterized by having the coupling means which combines and outputs the description data by which the feature extraction was carried out with said feature-extraction means, and authentication data before taking out from the original electronic filing document with authentication, and replacing with and inputting the output data from said coupling means into said description data as a candidate for encryption of said encryption means.

[Claim 25] From the changed electronic filing document containing the modification part data with authentication generated by the authentication means indicated by any or the 1st term said claim 21 thru/or among 24, and an electronic filing document with authentication The separation means which takes out said modification part data with authentication, and said electronic filing document with authentication, the document modification means indicated by any or the 1st term said claim 21 thru/or among 24, and difference -- with an extract means, a modification person authentication means, and an authentication means The alteration prevention system of the electronic filing document characterized by having the coupling means which generates a new changed electronic filing document based on the new modification part data with authentication and the new new electronic filing document with authentication which were generated by said authentication means, and the modification part data with authentication of the origin separated with said separation means.

[Claim 26] An acceptance means to receive each data attested by said modification person authentication means indicated by any or the 1st term said claim 21 thru/or among 24, The coupling means which combines the date data and authentication activation identification information with said each of each data at least, The external authentication system of the electronic filing document characterized by having an encryption means to encipher each data combined by this coupling means by the cryptographic key of an external certificate authority, and to create the authentication data by which external authentication was carried out.

[Claim 27] The authentication-text document check system characterized by having a decryption means to decode the authentication data in which external authentication was carried out by said external authentication system according to claim 26 with the decode key of an external certificate authority, and the data fetch means which takes out said date data and said authentication activation identification information from the authentication data decoded by said decryption means.

[Claim 28] The authentication-text document check system according to claim 27 characterized by having the authentication data fetch means which takes out the authentication data of said before from the authentication data which the authentication data external authentication was carried out [data] by said external authentication system according to claim 26 corresponded to said claim 23, and were decoded by said decryption means when it was a thing corresponding to an electronic filing document.

[Claim 29] While the code data enciphered with the encryption means of said claim 22 among the authentication data decoded by said decryption means are inputted The 2nd decryption means which decodes the code data concerned with a modification person's decode key, and takes out the description data, A feature-extraction means to carry out a feature extraction from the new electronic filing document obtained with the document modification means of said claim 21, and to output the description data for a comparison, The authentication-text document check system according to claim 28 characterized by having a collating means to compare the description data obtained with said 2nd decryption means with the description data for a comparison obtained with said feature-extraction means.
[Claim 30] By the authentication data external authentication was carried out [data] by said external authentication system according to claim 26 corresponding to said claim 24, when it is a thing corresponding to an electronic filing document The 2nd decryption means which decodes the authentication data decoded by said decryption means with a modification person's decode key, The authentication-text document check system according to claim 27 characterized by having the authentication data fetch means which takes out the authentication data of said before from the authentication data decrypted with said 2nd decryption means.
[Claim 31] The authentication-text document check system according to claim 30 which characterizes by to have had the collating means compare the description data obtained from the authentication data decrypted with said 2nd decryption means with the separation means which takes out description data, a feature-extraction means carry out a feature extraction from the new electronic filing document obtained with the document modification means of said claim 21, and output the description data for a comparison, and said separation means with the description data for a comparison which were obtained with said feature-extraction means.
[Claim 32] By the authentication data external authentication was carried out [data] by said external authentication system according to claim 26 corresponding to said claim 22, when it is a thing corresponding to said modification part data While the code data enciphered with the encryption means of said claim 22 among said decrypted authentication data are inputted The 2nd decryption means which decodes the code data concerned with a modification person's decode key, and takes out the description data, the difference of said claim 21 -- with a feature-extraction means to carry out a feature extraction from the modification part data obtained with the extract means, and to output the description data for a comparison The authentication-text document check system according to claim 27 characterized by having a collating means to compare the description data obtained with said 2nd decryption means with the description data for a comparison obtained with said feature-extraction means.
[Claim 33] It is the system which performs the authentication check about the modification part of the changed electronic filing document drawn up by the alteration prevention system of the electronic filing document indicated by said claim 25. Said claim 28 or 30 authentication-text document check systems, While having the authentication-text document check system of said claim 32, from the electronic filing document with authentication in the final changed electronic filing document which received modification of multiple times Take out the authentication data about the last modification time, and this is first inputted into said claim 28 or the authentication-text document check system of 30 as authentication data in which external authentication was carried out by said external authentication system according to claim 26. About each time other than the last modification time, authentication data before [said] outputting from said claim 28 or the authentication-text document check system of 30 as authentication data in which external authentication was carried out by said external authentication system according to claim 26 It inputs into said claim 28 or the authentication-text document check system of 30 one by one. Again The modification part data with authentication of each time are taken out from the final changed electronic filing document which received modification of multiple times. This modification part data with authentication is divided into the authentication data in which external authentication was

carried out by modification part data and said external authentication system according to claim 26. The date data and authentication activation identification information which inputted into the authentication-text document check system of said claim 32, and were obtained from said claim 28 or the authentication-text document check system of 30, The authentication check system of the changed electronic filing document characterized by collating the date data and authentication activation identification information which were obtained from the authentication-text document check system of said claim 32 for every modification time.

[Claim 34] The authentication check system of the changed electronic filing document according to claim 33 characterized by replacing with said claim 28 or the authentication-text document check system of 30 the authentication data and the new electronic filing document which were taken out from the electronic filing document with authentication included by the final changed electronic filing document, and inputting them into said claim 29 or the authentication-text document check system of 31 while having said claim 29 or the authentication-text document check system of 31.

[Claim 35] An electronic filing document is taken out from an electronic filing document with authentication. To this modification In addition, a document modification means to generate a new electronic filing document, the difference which extracts the changed part of the electronic filing document of the origin taken out from said electronic filing document with authentication, and said new electronic filing document, and acquires modification part data -- with an extract means While sending out each data attested by the modification person authentication means which carries out modification person authentication of said modification part data and said new electronic filing document, respectively, and said modification person authentication means to an external authentication system Receive the authentication data by which external authentication was carried out in each, and based on each received authentication data and said new electronic filing document as an authentication means to generate modification part data with authentication, and a new electronic filing document with authentication The record medium which recorded the program for operating a computer and in which computer reading is possible.

[Claim 36] said modification person authentication means -- said modification part data -- and -- or the record medium according to claim 35 in which computer reading which recorded the program for operating a computer as a feature-extraction means carries out a feature extraction from said new electronic filing document, and output the description data, and an encryption means encipher and output said description data with the encryption key of the modification person who generated said new electronic filing document is possible.

[Claim 37] The record medium which recorded the program for operating a computer as a data fetch means which takes out said date data and said authentication activation identification information from the authentication data decoded by decryption means to decode the authentication data in which external authentication was carried out by said external authentication system according to claim 26 with the decode key of an external certificate authority, and said decryption means and in which computer reading is possible.

[Translation done.]

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention prevents the alteration of electronic filing documents, such as data and a document, and relates to the alteration prevention system and approach of an electronic filing document which have the description in the part which secures especially the weight of the evidence of an electronic filing document.
[0002]
[Description of the Prior Art] In order to prevent the doubt of a document alteration, black ink, a ball-point, etc. are used for the former to documents, such as a transaction register, quality record, or a contract, they fill them in in the paper, and are performing a signature and seal.
[0003] Thus, what was indicated in ink on paper cannot be easily altered, even if it is going to alter written contents and a date behind. If it becomes old, in order that quality may change, even if paper draws up a fake document newly, it can be distinguished. For the description of such paper and ink, all important documents are kept in paper from the former.
[0004] Recently, an electronic signature technique can be developed and he who drew up the document can be proved now. This electronic signature is explained.
[0005] Drawing 53 is drawing showing the conventional method of signing an electronic filing document and judging the identity.
[0006] As shown in this drawing, description data 203D is first taken out from electronic-filing-document 201a with the feature-extraction means 202. Next, this description data 203D is enciphered with the encryption means 205 using a private key 204, and code data 206D is created. And this code data 206D is made together with electronic-filing-document 201a of origin, and it transmits to a recipient as signed electronic-filing-document 201b.
[0007] A recipient takes out code data 206D from received electronic-filing-document 201b', and takes out description data 218D with the decryption means 217 using a transmitting person's public key 216. On the other hand, electronic-filing-document 201a' equivalent to electronic-filing-document 201a of origin is taken out from electronic-filing-document 201b', and the description data 221 are further taken out with the feature-extraction means 220. It checks that the description data 221 are collated with previous description data 218D and the previous collating means 22, and there is nothing to his electronic filing document a difference.
[0008] With such an electronic filing document, the document preparation person can check that he is him rightly. however, an implementer -- if it is him, it is possible to change a document [finishing / creation] freely. therefore, an implementer -- he can shift the date of a computer intentionally and may produce problems, such as ********, for the creation data of a document.
[0009] Here, in the "generation method of an electronic document processing system system and a digital signature" indicated by the Japanese-Patent-Application-No. No. 303773 [five to] official report, another author adds a partial change to the drawn-up document, and the authentication approach when making it a new document is indicated.
[0010] However, using the drawn-up electronic filing document as a voucher to those those and the interest of an except disagree, such as the author concerned with creation, cannot say that it is suitable from an alteration of evidence being attained, if it alters by the author concerned with creation conspiring. That is, the approach of a Japanese-Patent-Application-No. No. 303773 [five to] official report does not get used to making a document electronize as a voucher, but can be called electronization restricted when an in-house document was used in the company.

[0011] For example, according to the production process of a product, the person in charge for every process cannot apply to assembly record which sets its hand and seal to its process in its duty, but has become employment in paper. Moreover, also when setting its hand and seal to a record sheet by adding the check result of several lines by record of a periodic check, it had become employment in paper. In the electronic filing document which can be altered if such an object needs to make inspection records proof and conspires against them to the accident of product safety, proof is because it could not become.

[0012]

[Problem(s) to be Solved by the Invention] thus, a document preparation person -- since he can perform a document alteration, he cannot prove that he is not altering electronic filing documents, such as a transaction register, quality record, or a contract. For this reason, in the present system, the credibility over an electronic filing document is low, and the important document is dealt with in paper as usual.

[0013] However, the document of paper needs many locations for storage, and taking out a required document takes time amount. Moreover, when sending far away and there is the need of having the same weight of the evidence as our paper, there is a problem which does not have an approach besides sending our paper.

[0014] It is more convenient to keep it as an electronic filing document on the other hand, rather than it keeps it in the form of paper if a document comes to be drawn up with a word processor etc. by development of the latest computer. for example, the retrieval of a required document which does not take a storage area is easy -- etc. -- since it has an advantage -- it is -- this sake -- the electronization of a document -- society -- generally it progresses and is coming.

[0015] However, since the weight of the evidence of an electronic filing document is insufficient as described above, even if electronization of an important document is not made but it electronizes, the paper document which has weight of the evidence will be required separately as our paper. for this reason, the storage area about an important document is required -- etc. -- a problem is not still solved.

[0016] This invention aims at offering the alteration prevention system and approach of an electronic filing document that it makes it possible to promote the electronization of the document in true semantics, as a result reduction of the storage areas of a document, increase in efficiency of retrieval of a document, instant delivery to the distant place of the document of our paper, etc. can be realized while it was made in consideration of such the actual condition and gives the weight of the evidence which is originally the description of a paper document to an electronic filing document.

[0017] Moreover, other purposes of this invention are to abolish the need of re-recognizing a modification document by all persons concerned, and prevent a document alteration, and offer the alteration prevention system and approach of an electronic filing document whose creation of the electronic filing document which has the weight of the evidence more than the weight of the evidence of a paper document was enabled, even when two or more persons draw up one electronic filing document over a term at two or more:00.

[0018]

[Means for Solving the Problem] The main point of this invention is in the place which uses the code data which enciphered the description data extracted from the electronic filing document by the cryptographic key of the 1st person concerned, enciphered this enciphered description data by an external authentication person's cryptographic key further, and were obtained as a result as authentication data of an electronic filing document.

[0019] Thus, the authentication data obtained cannot be altered by others and cannot be altered by the malicious external authentication person to whom the enciphered description data were passed, either. That is, since the code of the 1st person concerned can be kicked to the description data itself, if an external authentication person alters this, it will be detected that an electronic filing document is not just. Furthermore, it becomes impossible to alter the authentication data by which external

authentication was carried out once also by him the 1st person concerned for encryption by the external authentication person.
[0020] On the other hand, when the electronic filing document of a basis is altered, the fact of the alteration is detected by the comparison with the description data from an alteration electronic filing document, and the description data contained in authentication data.
[0021] Thus, in this invention, if an electronic filing document or authentication data is altered in which phase even if it is [not to mention] the case of malice where it is further based on any of a malicious external authentication person, the 1st person concerned when based on malicious others, even if it is the case where an alteration is performed in which phase, the alteration fact will be detected.
[0022] Moreover, more specifically, solution of the above-mentioned technical problem is realized by the following solution means.
[0023] First, a feature-extraction means for invention corresponding to claim 1 to extract the description from an electronic filing document, and to generate the description data, The 1st encryption means which enciphers the description data by the 1st cryptographic key, and generates the 1st encryption data, It is the alteration prevention system of an electronic filing document equipped with the 2nd encryption means which adds external authentication data to the 1st encryption data, enciphers this by the 2nd cryptographic key, and generates the 2nd encryption data, and the means which uses the 2nd encryption data as the authentication data of an electronic filing document.
[0024] Since this invention established such a means, while giving the weight of the evidence which is originally the description of a paper document to an electronic filing document, it can make it possible to promote the electronization of the document in true semantics, as a result reduction of the storage areas of a document, increase in efficiency of retrieval of a document, instant delivery to the distant place of the document of our paper, etc. can be realized.
[0025] Next, a feature-extraction means for invention corresponding to claim 2 to extract the description from an electronic filing document, and to generate the description data, The 1st encryption means which enciphers the description data by the 1st cryptographic key, and generates the 1st encryption data, The document authentication system equipped with the 1st means of communications which receives authentication data, and a means to make authentication data correspond to an electronic filing document while transmitting the 1st encryption data, The external authentication data which contain the date in the 1st encryption data transmitted in the 1st means of communications at least are added. The 2nd encryption means which enciphers this by the 2nd cryptographic key and generates the 2nd encryption data, And while receiving the 1st encryption data, it is the alteration prevention system of the electronic filing document equipped with the external authentication system equipped with the 2nd means of communications which transmits to a document authentication system by using the 2nd encryption data as authentication data.
[0026] Since this invention established such a means, the same effectiveness as invention of claim 1 is acquired, and also an authentication data origination activity can be advanced to convenience and a short time in between with the 1st person concerned and an external authentication person by using a communication line.
[0027] Next, invention corresponding to claim 3 is set to claim 1 or invention corresponding to 2. It has the 3rd encryption means which enciphers the 1st encryption data by the 3rd cryptographic key, and generates the 3rd encryption data. The 2nd encryption means It is the alteration prevention system of the electronic filing document which replaces with the 1st encryption data, adds external authentication data to the 3rd encryption data, enciphers by the 2nd cryptographic key, and generates the 2nd encryption data.
[0028] Since such a means was established, the same effectiveness as invention of claim 1 is acquired, and also this invention can add encryption by the cryptographic key of the 2nd person concerned to authentication data, and can make this electronic filing document electronic inclination **** which becomes authentication of three persons of the 1st person concerned, the 2nd person concerned, and

an external authentication person.
[0029] Next, invention corresponding to claim 4 is the alteration prevention system of an electronic filing document equipped with the 4th encryption ****** which the 2nd cryptographic key enciphers the 2nd encryption data by the 4th different cryptographic key, generates the 4th encryption data, and is used as authentication data in invention corresponding to claims 1-3.
[0030] Since this invention established such a means, it passes through a long period of time, for example from authentication data origination. Even when possibility that the code will be decoded by advance of a technique arises About the 2nd encryption data generated among claims 1-3 by the alteration prevention system of an electronic filing document any or given in 1 term, the reconfirmation certificate of the external authentication person by encryption for the second time can be performed, and the defense nature to the alteration of an electronic filing document can be maintained.
[0031] Next, the 2nd decryption means which invention corresponding to claim 5 picks out the 2nd encryption data from the authentication data corresponding to the electronic filing document for authentication, and decrypts this with the 2nd public key corresponding to the 2nd cryptographic key, The 1st decryption means which picks out the 1st encryption data from the data decrypted by the 2nd decryption means, and decrypts this with the 1st public key corresponding to the 1st cryptographic key, It is the authentication-text document check system equipped with a feature-extraction means to extract the description from an electronic filing document and to generate the description data for enquiry, and a collating means to pick out the description data from the data decrypted by the 1st decryption means, and to collate with the description data for enquiry.
[0032] Since this invention established such a means, while checking the authentication fact and an authentication day about the electronic filing document to which the weight of the evidence which is originally the description of a paper document was given, the system which can contribute to promoting the electronization of the document in true semantics can be offered. Thereby, if it pulls, reduction of the storage areas of a document, the increase in efficiency of retrieval of a document, the instant delivery to the distant place of the document of our paper, etc. are realizable.
[0033] Next, invention corresponding to claim 6 is set to invention corresponding to claim 5. The 3rd encryption data is picked out from the data decrypted by the 2nd decryption means. The 3rd decryption means which decrypts this with the 3rd public key corresponding to the 3rd cryptographic key is established. The 1st decryption means is an authentication-text document check system which picks out the 1st encryption data from the data decrypted by the 3rd decryption means, and decrypts this with the 1st public key corresponding to the 1st cryptographic key.
[0034] Since this invention established such a means, the same effectiveness as invention of claim 5 can be acquired also about the electronic contract which mixed the 2nd person concerned.
[0035] Next, invention corresponding to claim 7 is beginning to read one unit of data for a feature extraction at a time. The 1st train generation means which puts the total value which comes to add only the number of unit of a convention of the read value in order in order one by one, and is made into the 1st total value train, The value used as the relation which separated only the regular number of unit to this value that it read at a time one unit which it read at a time one unit is added. The 2nd train generation means which adds the value which serves as relation to this added value, and which it read at a time one unit, repeats this addition, puts in order the total value acquired by adding a regular number-of-unit time as a count of adding one by one, and is made into the 2nd total value train, It is feature-extraction equipment equipped with a means to output the 1st total value train and the 2nd total value train as description data.
[0036] Since this invention established such a means, it can generate the description data which could not reproduce the electronic filing document of a basis, but could detect that when performing the alteration, and carried out the data compression of the electronic filing document of a basis sharply only from the description data obtained in this way.
[0037] Next, invention corresponding to claim 8 is set to invention corresponding to claim 7. reading

appearance of the one every unit of the 1st total value train being carried out, and with the 3rd train generation means which puts the total value which comes to add only the number of unit of a convention of the read value in order in order one by one, and is made into the 3rd total value train It is feature-extraction equipment equipped with the 4th train generation means which puts in order the total value which comes to add only the number of unit of a convention of the value which was beginning to read one unit of 2nd total value train at a time, and read it in order one by one, and is made into the 4th total value train, and a means to output the 3rd total value train and the 4th total value train as description data.

[0038] Since such a means was established, the same effectiveness as invention of claim 7 is acquired, and also this invention can compress the description data more.

[0039] Next, a fingerprint feature-extraction means for invention corresponding to claim 9 to perform a feature extraction from the fingerprint data read with the fingerprint reading means and the fingerprint reading means, and to generate the fingerprint description data, A cryptographic key generation means to generate a cryptographic key from the fingerprint description data and a password, A private key public key generation means to generate a private key and a public key from the fingerprint description data, a password, and a random-number value, the data, the fingerprint data, and the password which were enciphered with an encryption means to encipher the cryptographic key itself and a private key by the cryptographic key, respectively, and the encryption means -- him -- him having the means used as authentication data -- it is an authentication data generative system.

[0040] since this invention established such a means -- a fingerprint etc. -- using -- effective him -- authentication data can be created. in addition, him who created by this system -- authentication data -- for example, him at the time of starting of a document alteration prevention system and an authentication-text document check system -- it can consider as the data for a check.

[0041] next, him invention corresponding to claim 10 was indicated to be by claim 9 -- him who generated with the authentication data generative system -- with the password in authentication data When both passwords are in agreement with a password collating means to collate the entered password, and a fingerprint reading means a fingerprint reading means -- fingerprint reading -- carrying out -- him, when fingerprint authentication is in agreement with a fingerprint authentication means to collate the fingerprint data in authentication data, and the fingerprint data read with the fingerprint reading means A fingerprint feature-extraction means to perform a feature extraction from the fingerprint data of he authentication data Naka, and to generate the fingerprint description data, A cryptographic key generation means to generate a cryptographic key from the fingerprint description data generated with the fingerprint feature-extraction means, and a password, The cryptographic key as which it was enciphered in authentication data is decoded. this generated cryptographic key -- him -- the case where cryptographic key collating is in agreement with a cryptographic key collating means to collate the generated cryptographic key and the decoded cryptographic key -- this cryptographic key -- using -- him -- it is the private key decode system equipped with a private key decode means to decode the private key enciphered in authentication data.

[0042] Since this invention established such a means, he can be checked with high certainty, for example at the time of starting of a document alteration prevention system and an authentication-text document check system.

[0043] Next, invention corresponding to claim 11 is fingerprint data extraction equipment equipped with the fingerprint reading means, a boundary detection means detect the boundary of the fingerprint data read in a fingerprint reading means, the embossing means that carries out embossing processing of the fingerprint data by which boundary detection was carried out with the boundary detection means, and the profile trace means which carries out profile trace of the fingerprint data by which embossing processing was carried out with the embossing means.

[0044] Since this invention established such a means, a fingerprint can be extracted as digital data which can be treated by the calculating machine.

[0045] Next, the field fetch means which takes out two or more rectangle fields from the fingerprint data extracted from the fingerprint data extraction equipment with which invention corresponding to claim 12 was indicated by claim 11, A pattern-matching means to judge whether the data of a rectangle field are compared with two or more patterns registered beforehand, and it matches with which pattern, It is fingerprint feature-extraction equipment equipped with the means which puts the numeric value corresponding to the matched pattern in order as a sequence of numbers, and uses the sequence of numbers concerned as the fingerprint description data.
[0046] Since this invention established such a means, the fingerprint description data can be effectively extracted from fingerprint data.
[0047] Next, invention corresponding to claim 13 considers invention of claim 1 as approach invention, and does so the same effectiveness as invention of claim 1.
[0048] Next, invention corresponding to claim 14 considers invention of claim 2 as approach invention, and does so the same effectiveness as invention of claim 2.
[0049] Next, invention corresponding to claim 15 considers invention of claim 3 as approach invention, and does so the same effectiveness as invention of claim 3.
[0050] Invention corresponding to claim 16 the 2nd encryption data from the authentication data generated by the alteration prevention system of an electronic filing document according to claim 1, 2, or 3 Next, drawing, The 2nd decryption step which decrypts this with the 2nd public key corresponding to the 2nd private key, The 1st decryption step corresponding to drawing for the 1st encryption data decrypted from the data decrypted by the 2nd decryption step with the 1st public key corresponding to the 1st private key for this, The feature-extraction step which extracts the description from an electronic filing document and generates the description data for collating, The collating step which collates the description data with drawing from the data decrypted by the 1st decryption step, and collates this with the description data for collating, It is the authentication-text document symptom which has the step which outputs the fact of authentication by the external authentication person, and the date of authentication with the external authentication data picked out from the data decrypted by the collating result by the collating step, and the 2nd decryption means.
[0051] Since this invention established such a means, it does so the same effectiveness as invention of claim 5.
[0052] Next, invention corresponding to claim 17 is invention about a record medium which stored the program for realizing invention of claim 1, and the computer which performs this program does so the same operation effectiveness as the thing except the 2nd encryption means in invention of claim 1.
[0053] Invention corresponding to claim 18 the 2nd encryption data from the authentication data generated by the alteration prevention system of an electronic filing document according to claim 1, 2, or 3 Next, drawing, The 2nd decryption means which decrypts this with the 2nd public key corresponding to the 2nd private key, The 1st decryption means corresponding to drawing for the 1st encryption data decrypted from the data decrypted by the 2nd decryption means with the 1st public key corresponding to the 1st private key for this, A feature-extraction means to extract the description from an electronic filing document and to generate the description data for collating, A collating means to collate the description data with drawing from the data decrypted by the 1st decryption means, and to collate this with the description data for collating, With the external authentication data picked out from the data decrypted by the collating result by the collating means, and the 2nd decryption means It is the record medium which recorded the program for operating a computer as a means to output the fact of authentication by the external authentication person, and the date of authentication and in which computer reading is possible.
[0054] Since this invention established such a means, the computer which performs this program does so the same operation effectiveness as invention of claim 5.
[0055] Next, invention corresponding to claim 19 is invention about the record medium with which the DS acquired as a result by which processing in invention of claim 1 was performed was recorded.

[0056] Next, invention corresponding to claim 20 is invention about the record medium with which the DS acquired as a result by which processing in invention of claim 3 was performed was recorded.
[0057] Next, invention corresponding to claim 21 takes out an electronic filing document from an electronic filing document with authentication. this -- modification -- in addition, the difference which extracts the changed part of a document modification means to generate a new electronic filing document, and the electronic filing document of the origin taken out from the electronic filing document with authentication and a new electronic filing document, and acquires modification part data -- with an extract means While sending out each data attested by the modification person authentication means which carries out modification person authentication of modification part data and the new electronic filing document, respectively, and the modification person authentication means to an external authentication system The authentication data by which external authentication was carried out in each are received, and it is the alteration prevention system of the electronic filing document equipped with modification part data with authentication, and an authentication means to generate a new electronic filing document with authentication, based on each authentication data and the new electronic filing document which were received.
[0058] It can also attest the data of only a modification part and can prevent the alteration of a modification electronic filing document while it can do ****** which gives new authentication to the changed electronic filing document, since this invention established such a means. Moreover, since external authentication has been acquired, it is reliable.
[0059] next, invention corresponding to claim 21 in invention corresponding to claim 22 -- setting -- a modification person authentication means -- modification part data -- and -- or it is the alteration prevention system of the electronic filing document equipped with a feature-extraction means carries out a feature extraction from a new electronic filing document, and output the description data, and an encryption means encipher and output the description data with the encryption key of the modification person who generated a new electronic filing document.
[0060] since this invention established such a means -- modification part data -- and -- or safety can be raised, leaving the description of an attesting agency, in order to use as authentication data not the new electronic filing document itself but the thing which enciphered the description data. Furthermore, the amount of data of authentication data can be lessened.
[0061] Next, invention corresponding to claim 23 is the alteration prevention system of the electronic filing document equipped with the coupling means which a modification person authentication means is outputted from an encryption means, and combines and outputs the encryption description data corresponding to a new electronic filing document, and authentication data before taking out from the original electronic filing document with authentication in invention corresponding to claim 22.
[0062] Since this invention established such a means, it can include former authentication data in the ****** data given to the new electronic filing document after modification, and can make them the hysteresis for every modification. Moreover, the authentication data of each time can be held.
[0063] Next, invention corresponding to claim 24 is the alteration prevention system of an electronic filing document which a modification person authentication means is equipped with the coupling means which combines and outputs the description data by which the feature extraction was carried out with the feature-extraction means, and authentication data before taking out from the original electronic filing document with authentication, and replaces with and inputs the output data from a coupling means into the description data as a candidate for encryption of an encryption means in invention corresponding to claim 22.
[0064] Since this invention established such a means, the same effectiveness as invention corresponding to claim 23 is realizable by other technique.
[0065] next, invention corresponding to claim 25 from the changed electronic filing document containing the modification part data with authentication generated by the authentication means indicated by any or the 1st term claim 21 thru/or among 24, and an electronic filing document with authentication The

separation means which takes out modification part data with authentication, and an electronic filing document with authentication, the document modification means indicated by any or the 1st term claim 21 thru/or among 24, and difference -- with an extract means, a modification person authentication means, and an authentication means It is the alteration prevention system of the electronic filing document equipped with the coupling means which generates a new changed electronic filing document based on the new modification part data with authentication and the new new electronic filing document with authentication which were generated by the authentication means, and the modification part data with authentication of the origin separated with the separation means.

[0066] This invention can draw up the changed electronic filing document which can hold the authentication data for every modification, without increasing the electronic filing document after modification, even if there is modification of multiple times since such a means was established.

[0067] Next, an acceptance means to receive each data attested by modification person authentication means by which invention corresponding to claim 26 was indicated by any or the 1st term claim 21 thru/or among 24, The coupling means which combines the date data and authentication activation identification information with each of each data at least, It is the external authentication system of the electronic filing document equipped with an encryption means to encipher each data combined by this coupling means by the cryptographic key of an external certificate authority, and to create the authentication data by which external authentication was carried out.

[0068] Since this invention established such a means, certain and safe authentication of a modification electronic filing document can be performed.

[0069] Next, invention corresponding to claim 27 is the authentication-text document check system equipped with a decryption means to decode the authentication data in which external authentication was carried out by the external authentication system according to claim 26 with the decode key of an external certificate authority, and the data fetch means which takes out the date data and authentication activation identification information from the authentication data decoded by the decryption means.

[0070] Since this invention established such a means, it can acquire the authentication information (authentication activation ID etc.) in an authentication date and an external certificate authority.

[0071] Next, invention corresponding to claim 28 is the authentication-text document check system equipped with the authentication data fetch means which takes out former authentication data from the authentication data which the authentication data external authentication was carried out [data] by the external authentication system according to claim 26 corresponded to claim 23, and were decoded by the decryption means when it was a thing corresponding to an electronic filing document in invention corresponding to claim 27.

[0072] Since this invention established such a means, when modification authentication of multiple times is made, authentication data ****** of each time can take out external authentication information.

[0073] Next, while the code data enciphered with the encryption means of claim 22 in invention corresponding to claim 28 among the authentication data decoded by the decryption means are inputted, invention corresponding to claim 29 The 2nd decryption means which decodes the code data concerned with a modification person's decode key, and takes out the description data, A feature-extraction means to carry out a feature extraction from the new electronic filing document obtained with the document modification means of claim 21, and to output the description data for a comparison, It is the authentication-text document check system equipped with a collating means to compare the description data obtained with the 2nd decryption means with the description data for a comparison obtained with the feature-extraction means.

[0074] Shinsei [this invention / an electronic filing document] since this invention established such a means can be checked.

[0075] Next, invention corresponding to claim 30 is set to invention corresponding to claim 27. By the authentication data external authentication was carried out [data] by the external authentication

system according to claim 26 corresponding to claim 24, when it is a thing corresponding to an electronic filing document It is the authentication-text document check system equipped with the authentication data fetch means which takes out former authentication data from the authentication data decrypted with the 2nd decryption means which decodes the authentication data decoded by the decryption means with a modification person's decode key, and the 2nd decryption means.
[0076] Since this invention established such a means, the same effectiveness as invention corresponding to claim 28 can be acquired by other technique.
[0077] Next, invention corresponding to claim 31 is set to invention corresponding to claim 30. The separation means which picks out the description data from the authentication data decrypted with the 2nd decryption means, It is the authentication-text document check system equipped with a collating means to compare a feature-extraction means to carry out a feature extraction from the new electronic filing document obtained with the document modification means of claim 21, and to output the description data for a comparison, and the description data obtained with the separation means with the description data for a comparison obtained with the feature-extraction means.
[0078] Since this invention established such a means, the same effectiveness as invention corresponding to claim 29 can be acquired by other technique.
[0079] Next, invention corresponding to claim 32 is set to invention corresponding to claim 27. By the authentication data external authentication was carried out [data] by the external authentication system according to claim 26 corresponding to claim 22, when it is a thing corresponding to modification part data While the code data enciphered with the encryption means of claim 22 among the decrypted authentication data are inputted The 2nd decryption means which decodes the code data concerned with a modification person's decode key, and takes out the description data, the difference of claim 21 -- with a feature-extraction means to carry out a feature extraction from the modification part data obtained with the extract means, and to output the description data for a comparison It is the authentication-text document check system equipped with a collating means to compare the description data obtained with the 2nd decryption means with the description data for a comparison obtained with the feature-extraction means.
[0080] Since this invention established such a means, the justification of the modification part data in each time can be checked, as a result Shinsei [an electronic filing document] can be checked.
[0081] Next, invention corresponding to claim 33 is a system which performs the authentication check about the modification part of the changed electronic filing document drawn up by the alteration prevention system of the electronic filing document indicated by claim 25. While having claim 28 or the authentication-text document check system of 30, and the authentication-text document check system of claim 32 From the electronic filing document with authentication in the final changed electronic filing document which received modification of multiple times Take out the authentication data about the last modification time, and this is first inputted into claim 28 or the authentication-text document check system of 30 as authentication data in which external authentication was carried out by the external authentication system according to claim 26. About each time other than the last modification time, authentication data before outputting from claim 28 or the authentication-text document check system of 30 as authentication data in which external authentication was carried out by the external authentication system according to claim 26 It inputs into claim 28 or the authentication-text document check system of 30 one by one. Again The modification part data with authentication of each time are taken out from the final changed electronic filing document which received modification of multiple times. This modification part data with authentication is divided into the authentication data in which external authentication was carried out by modification part data and the external authentication system according to claim 26. The date data and authentication activation identification information which inputted into the authentication-text document check system of claim 32, and were obtained from claim 28 or the authentication-text document check system of 30, It is the authentication check system of the changed electronic filing document which collates the date data and authentication activation

identification information which were obtained from the authentication-text document check system of claim 32 for every modification time.
[0082] Since this invention established such a means, it can check the truth of a changed electronic filing document, and enables use as a proof.
[0083] Next, in invention corresponding to claim 33, invention corresponding to claim 34 is an authentication check system of a changed electronic filing document which replaces with claim 28 or the authentication-text document check system of 30 the authentication data and the new electronic filing document which were taken out from the electronic filing document with authentication included by the final changed electronic filing document, and inputs them into claim 29 or the authentication-text document check system of 31 while being equipped with claim 29 or the authentication-text document check system of 31.
[0084] Since this invention established such a means, it can heighten the weight of the evidence of an electronic filing document further.
[0085] Next, invention corresponding to claim 35 is the record medium which recorded the program which makes a computer realize invention corresponding to claim 21.
[0086] The computer controlled by the program read from this record medium functions as an alteration prevention system of the electronic filing document of claim 21.
[0087] Next, invention corresponding to claim 36 is the record medium which recorded the program which makes a computer realize invention corresponding to claim 22.
[0088] The computer controlled by the program read from this record medium functions as an alteration prevention system of the electronic filing document of claim 22.
[0089] Next, invention corresponding to claim 37 is the record medium which recorded the program which makes a computer realize invention corresponding to claim 27.
[0090] The computer controlled by the program read from this record medium functions as an alteration prevention system of the authentication-text document check system electronic filing document of claim 27.
[0091]
[Embodiment of the Invention] Next, the gestalt of operation of this invention is explained.
[0092] [-- the 1- explanation] drawing 1 about the 13th operation gestalt is drawing showing the overall configuration of the alteration prevention system of the electronic filing document in each operation gestalt of this invention, and an approach.
[0093] The network 100 using a public line or a dedicated line is constituted, and the document authentication system 101, the external authentication system 102 of the external certificate authority 99, and the authentication-text document check system 103 are connected to the network concerned.
[0094] The document authentication system 101 sends the predetermined information on the system user creation concerned about the electronic filing document used as the candidate for authentication (a kind of user authentication by having enciphered with a user's key is included) to the external authentication system 102 through a network 100, receives the reply of the information for the authentication created by the external authentication system 102 based on this predetermined information, and draws up an authentication electronic filing document. Moreover, although a next operation gestalt also explains, the predetermined information processed by system user who is different by two or more document authentication systems 101, respectively (it is encryption, authentication information addition, etc. and has become the substantial authentication by each user) may be sent to the external authentication system 102.
[0095] On the other hand, the authentication-text document check system 103 is a system for checking the justification of the above-mentioned authentication electronic filing document, and receives the authentication electronic filing document for a check from document authentication system 101 grade through a network 100.
[0096] The document authentication system 101, the external authentication system 102, and the

authentication-text document check system 103 add for example, a display, an input unit, or a fingerprint reader to computers, such as a workstation and a personal computer, and each function which is different because the program of operation is fundamentally different is realized. Therefore, as shown in drawing 1 , the document authentication system 101 and the authentication-text document check system 103 may be constituted on the same computer.
[0097] Furthermore, it is also possible for it to be made to constitute on the computer to which the document authentication system 101 and the external authentication system 102 are connected by the same computer or LAN, and to be made to perform all the authentications in an external certificate authority.
[0098] The alteration prevention system and approach of an electronic filing document in connection with this invention combine suitably these document authentication systems 101, the external authentication system 102, and the authentication-text document check system 103, or are the thing which comes to combine a function in part suitably.
[0099] Moreover, although the case where it is premised on an instant transfer of the information through a network in the above-mentioned case is explained, as shown in drawing 1 R> 1, it is also possible to exchange required information (predetermined information and electronic filing document) through the record media 97 and 98, such as a floppy disk, between the document authentication system 101 - the external authentication system 102 or between the document authentication system 101 - the authentication-text document check system 103.
[0100] About the alteration prevention system and approach of an electronic filing document of on the whole having the above system configuration, each of that operation gestalt is explained below.
[0101] (Gestalt of the 1st operation) This operation gestalt is related with the creation system and approach of an electronic filing document that an alteration can be prevented.
[0102] Drawing 2 is the block diagram showing the example of a hardware configuration of the document authentication system applied to the alteration prevention system of the electronic filing document concerning the gestalt of operation of the 1st of this invention.
[0103] As for the document authentication system, it has come to connect a display 111, an input unit 112, an airline printer 113, external storage 114, the fingerprint reader 64, and a scanner 115 with a computer 110.
[0104] In the calculating machine 110, CPU117, ROM118, and RAM119 are connected to the CPU bus 116, and a hard disk drive unit 128, a communication device 121, a display 111, an input unit 112, an airline printer 113, external storage 114, the fingerprint reader 64, and the scanner 115 are further connected through each interface means 120, 121, 122, 123, and 124,125,126,127 connected to the CPU bus 116, respectively.
[0105] The boot processing program used for ROM118 starting a computer 110 and starting an operating system (OS) etc. is stored.
[0106] Moreover, the program storing section 130 and the data storage section 131 are formed in the hard disk drive unit 128. The program storing section 130 stores OS, the program which realizes the document authentication system 101, and the data storage section 131 stores an electronic filing document, an electronic filing document with authentication, and other various information.
[0107] RAM119 is used for the so-called primary storage. That is, the document authentication program 133 which is equipped with the working area 132 for the various processings by CPU117, and controls CPU117 is stored.
[0108] This document authentication program 133 is called from the program storing section 130 of a hard disk drive unit 128, and is stored in RAM119.
[0109] CPU117 controls each part according to the document authentication program 133 in RAM119, and realizes the document authentication system 101. That is, the software resource of RAM119 (especially document authentication program 133) or hard disk drive unit 128 grade and the hardware resources of drawing 2 of CPU117 grade join together, and each functional implementation means of the

document authentication system 101 is constituted. Each means (each processing) or each means (each processing) which is not illustrated expressed by a processing explanatory view, a flow chart, etc. in this operation gestalt and each following operation gestalt is such a functional implementation means, and is based on actuation of CPU117 which mainly follows the document authentication program 133.
[0110] A communication device 129 performs the communication link of the external authentication system 102, between, or the authentication-text document check system 103 and between. Transfer of an electronic filing document or various information is performed.
[0111] External storage 114 stores an electronic filing document, an electronic filing document with authentication, and other various information in a portability record medium, and makes preservation of an electronic filing document with authentication, sending, etc. conveniently and easy especially. As external storage 114, a floppy disk drive unit, optical-magnetic disc equipment (MO), CD-R, CD-R/W, or DVD is used, for example.
[0112] The fingerprint reader 64 is equipment which reads human being's fingerprint information. It is used for a system user's authentication, coding information creation, etc.
[0113] A scanner 115 is equipment which reads the graphic form of seal etc. as image information.
[0114] Next, the hardware configuration of an external authentication system is explained.
[0115] Drawing 3 is the block diagram showing the example of a hardware configuration of the external authentication system applied to the alteration prevention system of the electronic filing document of this operation gestalt, gives the same sign to the same part as drawing 2 , and omits the explanation.
[0116] The external authentication system 102 consists of the same computing systems as the document authentication system 101. The difference with the document authentication system 101 is a program of operation stored in the program storing section 130 of a hard disk drive unit 128. This program of operation is called and it is stored as an external authentication program 134 in RAM119. CPU117 controls each part according to this external authentication program 134, and the external authentication system 102 is realized. Moreover, the point that a software resource (especially external authentication program 134) and hardware resources join together, and a functional implementation means is constituted is the same as that of the case of the document authentication system 101.
[0117] Next, each function of the alteration prevention system of an electronic filing document is explained using drawing 4 . Drawing 4 is drawing showing the functional configuration of the alteration prevention system of the electronic filing document of this operation gestalt, and an example of processing flow.
[0118] The alteration prevention system of this electronic filing document consists of a document authentication system 101 and an external authentication system 102.
[0119] The document authentication system 101 gives complex data 10 to reception from the external authentication system 102 of the external certificate authority which gives authentication about this encryption data 6, gives this to the above-mentioned electronic filing document 1, and draws up the electronic filing document 12 with authentication while it extracts description data 3D from the electronic filing document 1 which should be attested and enciphers.
[0120] The document authentication system 101 For this reason, the fetch edit means of header 3H (not shown), It is [a feature-extraction means 2 to perform a feature extraction from an electronic filing document 1, and to generate description data 3D, and] the 1st private key 4 (#1) (to the configuration of the same kind and the data which may exist, hereafter) about description data 3D. An encryption means 6 to have described it as #1, #2, .., or the 1st .. [2nd] by the case, to have distinguished, to encipher, and to generate encryption data 6D (#1), A means (not shown) to combine header 3H and encryption data 6D, and the means of communications which transmits the combined encryption data 6 with a header to the external authentication system 102 (not shown), It has a means (not shown) to give the complex data 11 received from the external authentication system 102 to an electronic filing document 1, to draw up the electronic filing document 12 with authentication, and to save at electronic media.

[0121] On the other hand, the external authentication system 102 separates the code data 6 with a header received from the document authentication system 101 with a separation means (not shown). After giving external authentication data 7A (#1) to code data 7D of these and enciphering this with the 2nd private key 8 (#2) using the encryption means 9, This complex data 10 that serves as code data 10D from header 10H is combined by the coupling means (not shown), and it transmits to the document authentication system 101 by means of communications (not shown).
[0122] In addition, although the RSA method which used the private key and the public key as each data encryption method is used with this operation gestalt, other cipher systems (DES method etc.) may be used.
[0123] Next, actuation of the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained using drawing 4 and drawing 5 .
[0124] Drawing 5 is the flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[0125] First, the data of an electronic filing document 1 are read in the document authentication system 101 (S1), the part which can be used for data of header 3H, such as a document title and a date, is taken out from the document data, and in order to add supplementary information further, the line of the edit is carried out. In this way, a header 3 is created (S2). In addition, electronic seal, electronic signature, etc. of the document preparation person who explains for example, with the 7th operation gestalt are included in a header 3.
[0126] Next, the description is extracted from an electronic filing document 1 by the feature-extraction means 2, and description data 3D is created (S3). Here, description data 3D is data in which the description of the electronic filing document itself it is featureless to a value which is different even if 1 bit of an electronic filing document changed is shown. On the other hand, header 3H are data added in order to make it turn out of which electronic filing document description data 3D is a thing. As for header 3H and description data 3D, correspondence is taken as complex data (the description data 3 with a header).
[0127] Next, a private key 4 (#1) is used by the encryption means 5, description data 3D is enciphered, and 1st code data 6D is generated (S4). In addition, the 1st private key 4 is a private key which the implementer of an electronic filing document 1 holds, and it is made not to tell others about it.
[0128] Next, header 6H and code data 6D are combined, and correspondence is taken as code data 6 with a header (S5). In addition, header 6H are the same as header 3H. Thus, the made code data 6 with a header are transmitted to the external authentication system 102 of an external certificate authority (S6). In addition, although this transmission is transmitted to a network 100 through a public line or a dedicated line with this operation gestalt, it may be recorded, for example on electronic media, such as a floppy disk, and mailing etc. may carry out it.
[0129] On the other hand, in an external certificate authority, the code data 6 with a header from the document authentication system 101 are received (S7).
[0130] The code data 6 with a header are disassembled into header 7H and code data 7D in the external authentication system 102 (S8). External authentication data 7A is combined with code data 7D of these (S9). It is the information which shows what the external certificate authority which is a third person attested this external authentication data 7A for about the data with which the document authentication system 101 has required authentication, and the attested date data are contained.
[0131] Next, 1st code data 7D (#1) and external authentication data 7A (#1) are summarized by the encryption means 9, and it is enciphered with a private key 8 (S10). In this way, the 2nd code data 10D#2 is generated. Thereby, 2nd code data 10D (#2) serves as data by which the duplex was locked with an implementer's private key 4 and the private key 8 of an external certificate authority, and respectively original data are contained.
[0132] Furthermore, 2nd code data 10D is compounded with header 10H, and serves as complex data 10,

and the handling becomes a form easily (S11). In addition, header 10H are the same contents as header 3H. And complex data 10 is answered by the document authentication system 101 of the implementer who demands a third party certificate through a network 100 from the external authentication system 102 (S12).

[0133] In the document authentication system 101, complex data 10 is received as complex data 11 (S13). And this complex data 11 is compounded with an electronic filing document 1, and the electronic filing document 12 with authentication is generated. Data handling will become easy if such association is carried out. The generated electronic filing document 12 with authentication can be kept to the electronic media of the location of arbitration, and an authentication function will be demonstrated even if kept in which location. In addition, association here only includes various cases, when recording complex data 11 and an electronic filing document 1 on the same record medium, or when creating other data which show both correlation. This means to join together is also an example of the means used as the authentication data of the electronic filing document in a claim.

[0134] As mentioned above, when the alteration prevention system and approach of an electronic filing document concerning the gestalt of operation of this invention complete the procedure in which an external certificate authority attests the document in which electronic signature was done by him, it is proved by the authentication date of an external certificate authority that he was drawing up the document surely. moreover -- even if it is the case where there is no electronic signature even if -- a document preparation person -- the description data encryption should do with his private key 4 -- since it will be decrypted with the public key corresponding to this, it is attested that it is the document which becomes a document preparation person's creation anyway.

[0135] Moreover, if the body of a document is altered, the description data which should be extracted from the document after an alteration will change, and the fact of an alteration of a former document can be detected by becoming a different thing from description data 3D previously extracted for authentication. On the other hand, since description data 3D previously extracted for authentication is enciphered with the private key 8 of a certificate authority with authentication data 7A of an external certificate authority, the alteration of code data 11D given to the electronic filing document 12 with authentication is impossible. Therefore, even if it is him, after external authentication, a document alteration will become impossible.

[0136] The electronic filing document with weight of the evidence which can prove the justification of a document by this at the place of a trial can be generated, and it becomes possible the important document conventionally saved in paper, and to electronize a voucher. Moreover, although the advanced technique was needed for the document of the conventional paper judging the existence of an alteration, since the existence of an alteration can be checked only by completing an electronic procedure in the alteration prevention system of an electronic filing document which becomes this invention, the existence of an alteration can be proved easily. While storage areas are furthermore reduced by electronization, the document electrical transmission to a remote place can carry out now in an instant, and retrieval by the computer can be performed. In this way, improvement in trust of a commercial transaction and speeding up of dealings can be attained.

[0137] Moreover, since an electrical transmission data encryption is performed in the document authentication system 101 or the external authentication system 102 in the document alteration prevention system of this operation gestalt, respectively, it is safe even if it uses a public line as a network 100.

[0138] Furthermore, since the external authentication data which the external certificate authority attested are combined with the original electronic filing document and it was made to manage in the form of the electronic filing document 12 with authentication, the treatment when saving an electronic filing document becomes easy.

[0139] (Gestalt of the 2nd operation) This operation gestalt explains the system which takes out authentication information, such as an authentication date which checked Shinsei [the electronic filing

document 12 with authentication attested with the 1st operation gestalt], and the external certificate authority attached.
[0140] The alteration prevention system of this electronic filing document is constituted as an authentication-text document check system 103 shown in drawing 1 .
[0141] Drawing 6 is the block diagram showing the example of a hardware configuration of the authentication-text document check system applied to the alteration prevention system of the electronic filing document concerning the gestalt of operation of the 2nd of this invention, gives the same sign to the same part as drawing 2 , and omits the explanation.
[0142] The authentication-text document check system 103 consists of a document authentication system 101 and same computing system. The difference with the document authentication system 101 is a program of operation stored in the program storing section 130 of a hard disk drive unit 128. This program of operation is called and it is stored as an authentication-text document check program 135 in RAM119. CPU117 controls each part according to this authentication-text document check program 135, and the authentication-text document check system 103 is realized. Moreover, the point that a software resource (especially authentication-text document check program 135) and hardware resources join together, and a functional implementation means is constituted is the same as that of the case of the document authentication system 101.
[0143] Next, each function of the alteration prevention system of an electronic filing document is explained using drawing 7 . Drawing 7 is drawing showing the functional configuration of the authentication-text document check system 103 applied to the alteration prevention system of the electronic filing document of this operation gestalt, and an example of processing flow, gives the same sign to the same part as drawing 4 , and omits explanation.
[0144] This authentication-text document check system 103 collates the description data 21 extracted from the electronic filing document 19 which removed complex data 11 from description data 18D taken out from the electronic filing document 12 with authentication, and the electronic filing document 12 with authentication. While performing identity of an electronic filing document, the fact and its authentication date of authentication by the external certificate authority 99 are checked from external authentication data 15A taken out from authentication data (code data 11D).
[0145] for this reason, in the authentication-text document check system 103 The means which takes out header 11H and code data 11D from the electronic filing document 12 with authentication stored in external storage 114 or a hard disk drive unit 128 (not shown), A decryption means 14 to decrypt code data 11D with the 2nd public key 13 (#2) of the external authentication system 102, A means by which external authentication data 15A of the data obtained by this decryption (#1) performs an authentication check of date authentication 15 A-D and the external certificate authority 99 (not shown), A decryption means 17 to decrypt code data 15D of the data decrypted with the decryption means 14 with the 1st public key 16 (#1) of the document authentication system 101 is established. Furthermore, description data 18D taken out from the feature-extraction means 20 which takes out the description data 21 from the electronic filing document 19 which removed authentication data, this description data 21, and the description data 18 with a header decrypted with the decryption means 17 is collated, and a collating means to perform identity judging 22-J with an electronic filing document 19 the same as that of an electronic filing document 1 is established.
[0146] Although the RSA approach is used with this operation gestalt as a code which used the private key and the public key, other cipher systems (DES method etc.) may be used. In addition, an electronic filing document's 1 system or a third person's system of an implementer is sufficient as the authentication-text document check system 103 shown in drawing 7 .
[0147] Next, actuation of the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained using drawing 7 and drawing 8 .
[0148] Drawing 8 is the flow chart showing actuation of the alteration prevention system of the

electronic filing document of this operation gestalt.
[0149] First, an electronic filing document 12 is read through external storage 114 and a hard disk drive unit 128 to the network 100 (T1), and complex data 11 is taken out (T2).
[0150] 2nd code data 11D (#2) which functions as authentication data further out of complex data 11 is taken out (T3). Decode is performed by the decryption means 14 using the 2nd public key 13 (#2) (T four). In addition, the 2nd public key 13 (#2) is a public key of the external certificate authority 99, and is equivalent to the 2nd private key 8 (#2). 1st code data 15D (#1) and external authentication data 15A (#1) are taken out by this.
[0151] Next, code data 15D and external authentication data 15A are separated from the authentication data 15 with a header (T5). In addition, code data 15D has the same code data 6D and contents of drawing 4 . Moreover, external authentication data 15A has external authentication data 7A of drawing 4 , and the same contents. Furthermore, header data 15H have the same header data 3H and contents of drawing 4 .
[0152] Next, date authentication data 15 A-D is taken out from decoded external authentication data 15A, and the date with which the external certificate authority attested complex data 6 is checked (T6).
[0153] On the other hand, 1st code data 15D (#1) is decoded by the decryption means 17 with the 1st public key 16 (#1) (T6), and 1st description data 18D is generated. The 1st public key 16 (#1) is a public key of the implementer of an electronic filing document, and is equivalent to the 1st private key 4 (#1). In addition, description data 18D has the 1st same description data 3D (#1) and contents.
[0154] Next, the electronic filing document 19 excluding complex data 11 from the electronic filing document 12 is taken out (T8). This electronic filing document 19 corresponds to the original electronic filing document 1. Furthermore, the description data 21 are taken out from an electronic filing document 19 by the feature-extraction means 20 (T9). The feature-extraction means 20 is the same means as the feature-extraction means 2, and if the contents of the electronic filing document 19 are the same as that of an electronic filing document 1, the same description data will be generated.
[0155] Next, description data 18D and the description data 21 are collated by the collating means 22 (T10), and identity judging result 22-J which shows whether a collating result is the same is outputted. him who was attested under the date of date authentication data 15 A-D when identity judging result 22-J was judgment good (coincidence) (T11) -- it is proved that it is the document of creation. Then, the purport which is document identitas is displayed on a display 111 with the date authentication taken out at step T6 (T13).
[0156] On the other hand, an inequality will be displayed if identity judging result 22-J is a poor judgment (inequality) (T11).
[0157] As mentioned above, the alteration prevention system and approach of an electronic filing document concerning the gestalt of operation of this invention addition of the encryption description data, and him -- the external authentication data of an electronic filing document to the external certificate authority by which authentication of electronic signature and an external certificate authority was made -- drawing -- Moreover, it is proved by the authentication date of an external certificate authority by collating the description data and the description data from an electronic-filing-document body which are added using a document preparation person's public key 16 that he was drawing up the document surely.
[0158] If an electronic-filing-document body is altered, when the description data 21 extracted from an electronic filing document 19 change, even if 1st description data 3D and 18D are him by preventing an alteration by the external certificate authority 99, on the other hand after external authentication, a document alteration will become impossible. It becomes possible the important document which could prove the justification of a document by this at the place of a trial, and was conventionally saved in paper, and to electronize a voucher.
[0159] Moreover, although the advanced technique was needed for the document of the conventional paper judging the existence of an alteration, in the alteration prevention system of an electronic filing

document, the existence of an alteration can be easily proved by the above-mentioned collating processing. Furthermore, while storage areas are reduced by electronization, electrical transmission to a remote place can carry out through a network in an instant. Therefore, retrieval by the computer is also still more possible.

[0160] Moreover, since an electrical transmission data encryption is performed in the document authentication system 101 or the external authentication system 102 in the document alteration prevention system of this operation gestalt, respectively, it is safe even if it uses a public line as a network 100.

[0161] Furthermore, the treatment when saving a document becomes easy by combining with the original electronic filing document the authentication data which the external certificate authority attested.

[0162] (Gestalt of the 3rd operation) By the alteration prevention system and approach of an electronic filing document of this operation gestalt, external authentication data are further given to the complex data 11 given to the once drawn-up electronic filing document 12 with authentication, and encryption is applied again. The electronic filing document which strengthened alteration prevention by this is generated, and the secrecy nature of authentication data which passed through the long period of time from creation of the electronic filing document 12 with authentication is maintained.

[0163] Drawing 9 is drawing showing the functional configuration of the 3rd of the alteration prevention system of the electronic filing document of the gestalt of operation of this invention, and an example of processing flow, gives the same sign to the same part as drawing 4 and drawing 7 , and omits the explanation. Moreover, the document authentication system 101 and the external authentication system 102 which are shown in drawing 2 and drawing 3 are used for the system of this operation gestalt, and the original functional division of this operation gestalt is because correction was added to the document authentication program 133 or the external authentication program 134.

[0164] The alteration prevention system of this electronic filing document consists of the document authentication systems 101 and the external authentication systems 102 which are shown in drawing 1 .

[0165] A means by which the document authentication system 101 sends complex data 11 to drawing and the external authentication system 102 from an electronic filing document 12 (not shown), The means (not shown) which adds the code data 27 with a header received from the external authentication system 102 as authentication data to what removed the authentication data 11 from the electronic filing document 12, and was made into the original electronic filing document, and is made into the electronic filing document 28 with authentication is added, and also It is constituted like the 1st operation gestalt.

[0166] On the other hand, while the external authentication system 102 adds external authentication data 23A to complex data 11 from the document authentication system 101 An encryption means 25 to encipher code data 23D (the same as that of code data 11D), and external authentication data 23A with the 3rd private key 24 (#3), A means (not shown) to transmit this code data 26 with a header that serves as enciphered code data 26D from header 26H to the document authentication system 101 is added, and also it is constituted like the 1st operation gestalt. In addition, the 3rd private key 24 (#3) is another private key of the external certificate authority 99.

[0167] Next, actuation of the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained using drawing 9 and drawing 10 .

[0168] Drawing 10 is the flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.

[0169] First, in the document authentication system 101, an electronic filing document 12 is read through external storage 114 and a hard disk drive unit 128 to the network 100 (U1), and the complex data 11 which is authentication data is taken out (U2). This complex data 11 is transmitted to the external authentication system 102 of the external certificate authority 99 through a network 100 (U3).

[0170] .

[0171] Next, in the external authentication system 102, the complex data 11 (authentication data) transmitted at step U3 is received. Next, the received complex data 11 is divided into header 23D and code data 23D (U5). External authentication data 23A is added to the authentication data 23 with a header here. In addition, external authentication data 23A is the same as that of external authentication data 7A of the 1st operation gestalt, and information, such as an authentication day, is included.
[0172] Next, coincidence data 23D and external authentication data 23A are combined (U6), this joint data is enciphered with a private key 24 (#3), and code data 26D is generated (U7). In addition, this private key 24 is a private key of the external certificate authority 99, for example, corresponds to a RSA method.
[0173] Next, the code data 26 which are authentication data with which it comes to combine header 26H and coincidence data 26D are generated (U8), and the data 26 concerned are transmitted to the document authentication system 101 through a network 100 (U9).
[0174] The code data 26 transmitted from the external certificate authority 99 are received by the document authentication system 101 (U10). This is made into the code data 27 with a header, it is compounded by the electronic filing document of the origin which removed the code data 11 from the electronic filing document 12, and the electronic filing document 28 with authentication is generated (U11). In this way, the electronic filing document with which alteration prevention was strengthened will be generated. In addition, an electronic filing document 28 can be kept to the electronic media of the location of the arbitration of external storage 114, a hard disk drive unit 128, and others.
[0175] As mentioned above, since the alteration prevention system and approach of an electronic filing document concerning the gestalt of operation of this invention give authentication of the external certificate authority 99 again to the complex data 11 taken out from the electronic filing document 12, apply a code again and generated the electronic filing document 28 with authentication, they can draw up the document 28 which strengthened alteration prevention.
[0176] Therefore, before going through years with a possibility that the first code may be decoded, by advance of a code technique, even if it strengthens alteration prevention of a document 1 in a still newer code, and can carry out things and performs prolonged electronic-filing-document storage, the justification of a document can be proved at the place of a trial.
[0177] In addition, although this operation gestalt explained the case where the reconfirmation certificate of the electronic filing document of one authentication was carried out like an electronic filing document 12, it may be made to carry out the reconfirmation certificate of the electronic filing document 28 further using the technique of this operation gestalt. Thus, by repeating a reconfirmation certificate and piling up the count of authentication, the storage period of an electronic filing document 1 can be extended, and it can consider as infinity length as a matter of fact. therefore -- this operation gestalt -- the cipher system of a public key system (RSA) -- the time -- attesting -- a case -- having explained -- although -- each time -- developing -- having had -- decode is the most difficult -- a cipher system -- suitably -- a reconfirmation certificate (re-encryption) -- carrying out is appropriate.
[0178] (Gestalt of the 4th operation) This operation gestalt explains the system which takes out authentication information, such as each authentication date which checked Shinsei [the electronic filing document 28 with authentication which strengthened reconfirmation proof alteration prevention with the 3rd operation gestalt], and the external certificate authority attached.
[0179] Drawing 11 is drawing showing the functional configuration of the 4th of the alteration prevention system of the electronic filing document of the gestalt of operation of this invention, and an example of processing flow, gives the same sign to the same part as drawing 4 , drawing 7 , and drawing 9 , and omits the explanation. Moreover, the authentication-text document authentication system 103 shown in drawing 6 is used for the system of this operation gestalt, and the original functional division of this operation gestalt is because correction was added to the authentication-text document check program 135.
[0180] The alteration prevention system of this electronic filing document is constituted as an

authentication-text document check system 103 shown in drawing 1 .
[0181] The authentication-text document check system 103 is the process, and checks the purport of each authentication date and external authentication about two authentications by the external certificate authority 99 while it performs collating with the description data 21 which performed three decode processings about the authentication data taken out from the electronic filing document 28 with authentication, and took out description data 18D from drawing and an electronic filing document 19.
[0182] for this reason, in the authentication-text document check system 103 The means which takes out the code data 27 with a header from the electronic filing document 28 with authentication (not shown), A decryption means 30 to decrypt code data 27D with the public key 29 (#3) of the external certificate authority 99, The means (not shown) which performs an authentication check of the external certificate authority 99 from decrypted external authentication data 31A, and takes out date authentication 31 A-D is established, and also it is constituted like the 2nd operation gestalt shown in drawing 7 . In addition, the data which the decryption means 14 decodes are code data 31D.
[0183] Next, actuation of the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained using drawing 11 and drawing 12 .
[0184] Drawing 12 is the flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[0185] First, in the authentication-text document check system 103, the electronic filing document 28 with authentication is read through external storage 114 and a hard disk drive unit 128 to the network 100 (V1). Next, the code data 27 with a header which are authentication data are taken out from an electronic filing document 28 (V2). Furthermore, code data 27D is separated from the code data 27 with a header (V3). By the decryption means 30, this separated code data 27D is decrypted with the public key 29 (#3) of an external certificate authority (V4). The complex data of code data 31D and 2nd external authentication data 31A is generated by this. If there is no alteration in authentication data here, code data 31D is the same as code data 11D or 10D, and 2nd external authentication data 31A is the same as external authentication data 23A.
[0186] Next, code data 31D and 2nd external authentication data 31A are separated (V5). Furthermore, date authentication 31 A-D is taken out from external authentication data 31A, and authentication of this external certificate authority 99 that is the 2nd time is checked (V6). On the other hand, code data 31D is decoded by the decryption means 14 using the public key 13 (#2) of the external certificate authority 99, and the complex data of code data 15D and external authentication data 15A is generated (V7). If there is no alteration in authentication data here, code data 15D is the same as code data 6D or 7D, and external authentication data 15A is the same as 1st external authentication data 7A.
[0187] Next, the above-mentioned complex data is divided into external authentication data 15A and code data 15D (V8), and date authentication data 15 A-D is taken out from external authentication data 15A (V9). Thereby, authentication by the 1st external certificate authority 99 is checked.
[0188] Next, code data 15D is decrypted by the decryption means 17 using an implementer's public key 16 (#1), and the description data 18 with a header are generated (V10). Furthermore, it separates into header 18H and description data 18D (V11).
[0189] On the other hand, from the electronic filing document 28 with authentication, the code data 27 with a header take, and are **(ed), and the description data 21 are extracted from the electronic filing document 19 of the origin of this by the feature-extraction means 20 (V12). And description data 18D separated at step V11 and the description data 21 are collated by the collating means 22, and identity judging data 22-J is generated (V13).
[0190] When it is judged by identity judging data 22-J which it is as a result of collating whether an electronic filing document 19 and an electronic filing document 1 are the same (V14) and it is judged to be inharmonious, an inequality is displayed from a display 111 (V15). On the other hand, when it is judged that it is the same, authentication date 31 A-D and 15 A-D are displayed, and the display of the still

more nearly same purport is performed (V16). In this way, the identity judging of the electronic filing document which strengthened alteration prevention is completed.

[0191] As mentioned above, since the alteration prevention system and approach of an electronic filing document concerning the gestalt of operation of this invention set a period in the external certificate authority 99, collate identity about the electronic filing document 28 with authentication attested and enciphered over 2 times and checked external authentication, they can judge easily identity of the electronic filing document 28 which strengthened alteration prevention. Moreover, since alteration prevention of the document in a still newer code can be performed before going through years with fear of decryption, even if it performs prolonged electronic-filing-document storage, the justification of a document can be proved at the place of a trial.

[0192] Although this operation gestalt explained the example which performs one identity judging of the electronic filing document 28 of a reconfirmation certificate (a total of two external authentications) like an electronic filing document 28, the identity judging of the document which carried out the reconfirmation certificate of the electronic filing document 28 further may be carried out. When the count of authentication is piled up, the identity judging of an electronic filing document can be performed by piling up the count of decode.

[0193] (Gestalt of the 5th operation) This operation gestalt explains the electronic contract creation system using the alteration prevention system of an electronic filing document explained with the 1st or 3rd operation gestalt.

[0194] Drawing 13 is drawing showing the functional configuration of the 5th of the alteration prevention system of the electronic filing document of the gestalt of operation of this invention, and an example of processing flow, gives the same sign to the same part as drawing 4 , drawing 7 , drawing 9 , and drawing 11 , and omits the explanation. Moreover, the document authentication system 101 and the external authentication system 102 which are shown in drawing 2 and drawing 3 are used for the system of this operation gestalt, and the original functional division of this operation gestalt is because correction was added to the document authentication program 133 or the external authentication program 134.

[0195] The alteration prevention system of this electronic filing document consists of a document authentication system 101 (first system 101a is said hereafter) out of which a contractor comes on the other hand and which a certain first uses, a document authentication system 101 (second system 101b is said hereafter) which the second which is a contractor's another side uses, and an external authentication system 102. Moreover, the alteration prevention system of this electronic filing document is also an electronic contract creation system for performing the contract between A and B. In addition, as it is indicated in drawing 1 as the external authentication system 102, it connects with first system 101a and second system 101b in the network.

[0196] Using the private key 4 (first) of the first as a private key 4 (#1), first system 101a replaces the code data 6 with a header with the external authentication system 102, and transmits to second system 101b. Furthermore, give the code data 40 with a header to reception and an electronic filing document 1 as complex data 11 received from the external authentication system 102, and the electronic filing document 41 with authentication which is an electronic contract is drawn up, and also shell system 101a is constituted like the document authentication system 101 of the 1st or 3rd operation gestalt.

[0197] On the other hand, second system 101b generates the joint data which added authentication data 32A of the second to code data 32D in the code data 6 with a header received from first system 101a. A means (not shown) to create the authentication data 32 with a header, and an encryption means 34 to encipher this joint data with the private key 33 (second) of the second, A means to combine code data 35D enciphered with header 32H (35H) and the encryption means 34 of the authentication data 32 with a header, and to create electronic signature 35 (not shown), It has a means (not shown) to transmit this electronic signature 35 to an external authentication system through a network, and also is constituted like the document authentication system 101 of the 1st or 3rd operation gestalt.

[0198] In addition, first system 101a and second system 101b are good also as a system which

combines each function of each which gave [above-mentioned] explanation, and can perform the same processing.

[0199] Moreover, are constituted so that it may replace with the authentication data 7 with a header and the same processing as drawing 4 may be performed about the authentication data 36 with a header, and code data with a header are further transmitted to first system 101a instead of second system 101b, and also the external authentication system 102 is constituted like the 1st or 3rd operation gestalt. That is, in the authentication data 7 with a header of drawing 4 , and code data 36D, code data 7D of drawing 4 and external authentication data 36A correspond to external authentication data 7A of drawing 4 , and header 36H correspond [the authentication data 36 with a header] to header 7H of drawing 4 . Moreover, the code data 39 with a header correspond to the complex data 10 of drawing 4 , and, as for header 39H, header 10H of drawing 4 and code data 39D correspond to code data 10D of drawing 4 . Furthermore, the encryption means 38 is equivalent to the encryption means 9 of drawing 4 , and a private key 37 is equivalent to the private key 8 of drawing 4 . In addition, code data 36D is authentication data of the A and B which the first and the second were alike, respectively and were enciphered more, further, external authentication is given and the code data 39 are enciphered by the authentication data of these A and B.

[0200] Next, actuation of the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained using drawing 13 and drawing 14 .

[0201] Drawing 14 is the flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.

[0202] First, in shell system 101a, an electronic filing document 1 is read through external storage 114 and a hard disk drive unit 128 to the network 100 (W1). Next, a part for identification division is taken out from an electronic filing document 1, and a documentary stamp tax payment person name is filled in as amount-of-money information, in addition a need matter is edited, and it is referred to as header 3H (W2).

[0203] Next, description data 3D is extracted from an electronic filing document 1 by the feature-extraction means 2 (W3). Furthermore, description data 3D is enciphered by the encryption means 5 using the private key 4 (shell) of a contractor shell, and code data 6D is generated (W4). Header 3H (6H) and code data 6D are combined, and the code data 6 with a header which are electronic signature data of a contractor shell are generated (W5).

[0204] The electronic signature data of this contractor first are transmitted to second system 101b which the contractor second uses from first system 101a with an electronic filing document 1 (W6). In addition, when the second attests, an electronic filing document 1 is transmitted to the second, because the contents of a document can be checked.

[0205] In second system 101b, the electronic signature (code data 6 with a header) and electronic filing document 1 of the contractor first are received first (W7). This received electronic signature data is divided into header 32H and code data 32D (W8).

[0206] Next, authentication data 32A of the second is combined with code data 32D, and joint data are generated (W9). The identifier and date of the second are contained in this authentication data 32A. Next, code data 32D and authentication data 32A are enciphered by the encryption means 34 using the private key 33 of the second, and code data 35D is generated (W10).

[0207] And it becomes the first and the electronic signature 35 (code data 35 with a header) of the second by header 32H (35H) and code data 35D being combined (W11). Since the part enciphered with the private key 4 (first) of the first and the part enciphered with the private key 33 (second) of the second are contained and the identifier of A and B is further included in header 6H and authentication data 32A, this electronic signature 35 turns into both electronic signature substantially. Moreover, you may make it include the electronic signature of the normal of A and B in header 35H or code data 35D.

[0208] In this way, the electronic signature 35 of the generated first and the second is transmitted to

the external authentication system 102 of the external certificate authority 99 through a network 100 (W12).

[0209] The electronic signature 35 of the first and the second is received in the external authentication system 102 (W13). Next, the electronic signature 35 of the first and the second is divided into header 36H and code data 36D (W14). Furthermore, external authentication data 36A of an external certificate authority is combined with code data 36D (W15). The identifier of the external certificate authority 99, a date, and a report [finishing / documentary stamp tax payment] are contained in external authentication data 36A. About payment of documentary stamp tax, the shell contracts among the external certificate authorities 99 beforehand.

[0210] Next, code data 36D and authentication data 36A are enciphered by the encryption means 38 using the private key 37 of the external certificate authority 99, and code data 39D is generated (W16). Furthermore, header 36H (39H) and code data 39D are combined, and the code data 39 with a header which are the electronic signature of A and B and the external certificate authority 99 are completed (W17). This electronic signature is transmitted to shell system 101a via a network (W18).

[0211] In shell system 101a, the code data 39 with a header which are electronic signature are received as code data 40 with a header (W19). And the code data 40 with a header which are this electronic signature are compounded with an electronic filing document 1, and the electronic contract 41 (electronic filing document 41 with authentication) is completed.

[0212] As mentioned above, since the alteration prevention system and approach of an electronic filing document concerning the gestalt of operation of this invention give authentication about an electronic filing document 1 in the first, the second, and the external certificate authority 99, respectively and enciphered authentication data with each private key, they can prevent the alteration to the drawn-up electronic contract, and can make this an electronic filing document with weight of the evidence.

[0213] That is, if an electronic contract is altered that the description data which the electronic filing document 1 has when an electronic contract is altered change, and by enciphering description data 3D extracted by the beginning by a contractor's A and B and all the members of an external certificate authority, since it can surely discover, the contract in an electronic filing document is attained instead of paper. Furthermore, although the advanced technique was needed for judging the existence of an alteration by the document of the conventional paper, the existence of an alteration can be easily proved in the alteration prevention system of the **** document which becomes this invention. Moreover, while storage areas are reduced by electronization, electrical transmission to a remote place can carry out in an instant, and retrieval by the computer can be performed now.

[0214] In addition, in the contract of paper, in order to correct the error of a token, there was a bad habit which pushes an extra seal impression on a document, but by electronization, since an exchange of a document is attained among contractors in an instant, even if it does not push an extra seal impression on a document, it corrects immediately, and changes that a re-signature is possible, and generating of the trouble between contractors can be prevented. Since the contract price and the documentary stamp tax payment person name are indicated by electronic signature 35, there is no need of sending the electronic filing document itself to an external certificate authority, and an electronic contract can be used even when there is a matter to make it secret.

[0215] Moreover, in such a case, this invention is not restricted, although the description data are taken out from an electronic filing document 1 and authentication of A and B and an external certificate authority was given to this with this operation gestalt. For example, if description data 3D is taken out from the electronic filing document 1 to which the data with which a document preparation person's persons concerned and superior official are equivalent to the superior official mark etc. were added to electronic-filing-document 1 original the very thing, and the superior official mark concerned was added, it will become possible to take out the electronic filing document 1 to which the superior official's authentication was also given substantially. It is because the description data will change if the original electronic filing document is altered.

[0216] Furthermore, for example with this operation gestalt, although the case where a contractor was two persons, the first and the second, was explained, in such a case, this invention is not restricted. For example, when a contractor turns into three persons of the first, the second, and the third class, if it is made to be carried out repeatedly even if the step of the second in drawing 13 is attached to the third class, the same electronic contract as the above containing the authentication whose three persons are contractors can be drawn up. Moreover, what is necessary is just to carry out by repeating the step of this second, even if it is attached to **, when a contractor requires ** further. Therefore, it will not be concerned with a contractor's number, but an electronic contract can be drawn up and used for it.
[0217] (Gestalt of the 6th operation) This operation gestalt explains the system which takes out authentication information, such as each authentication date which checked Shinsei [the electronic contract drawn up with the 5th operation gestalt], and the contractor and the external certificate authority attached.
[0218] Drawing 15 is drawing showing the functional configuration of the 6th of the alteration prevention system of the electronic filing document of the gestalt of operation of this invention, and an example of processing flow, gives the same sign to the same part as drawing 4 , drawing 7 , drawing 9 , drawing 11 , and drawing 13 , and omits the explanation. Moreover, the authentication-text document authentication system 103 shown in drawing 6 is used for the system of this operation gestalt, and the original functional division of this operation gestalt is because correction was added to the authentication-text document check program 135.
[0219] The alteration prevention system of this electronic filing document is constituted as an authentication-text document check system 103 shown in drawing 1 , and is also a collating system of an electronic contract.
[0220] As opposed to the code data 40 with a header with which the authentication-text document check system 103 was given to the electronic contract 41 (electronic filing document 41 with authentication) The decode by the public key 42 (private seal) of the external certificate authority 99, the public key 45 (second) of the contractor second, and the public key 48 (first) of the contractor first is performed. While taking out the authentication fact and authentication date of the authentication fact of an external certificate authority and an authentication date, and the second and performing an authentication check Drawing and both the descriptions data 50 and 52 are collated [the description data 50] for the description data 52 from drawing and the electronic filing document 1 which, on the other hand, removed the code data 40 with a header, and an identity judging is performed.
[0221] for this reason, in the alteration prevention system of an electronic filing document The means which picks out the encryption data 40 with a header from the electronic contract 41 (not shown), A decryption means 43 to decode code data 40D contained in this with the public key 42 (private seal) of an external certificate authority, The means which takes out the authentication fact and authentication date of an external certificate authority from external authentication data 44A decrypted by the decryption means 43 as date authentication 44 A-D (not shown), A decryption means 46 to decrypt code data 44D decrypted by the decryption means 43 with the public key 45 (second) of the second is established. Furthermore, the authentication fact of the second, the means (not shown) which takes out an authentication date as date authentication 47 A-D, and a decryption means 49 to decrypt code data 47D decrypted by the decryption means 46 with the public key 48 (first) of the first are established from authentication data 47A of the second decrypted by the decryption means 46. A collating means 53 to collate a feature-extraction means 51 to perform a feature extraction on the other hand from the electronic filing document 1 of the origin by which the encryption data 40 with a header were removed from the electronic contract 41, and to generate the description data 52, and this description data 52 and description data 50D decrypted by the decryption means 49, and to perform identity judging 53-J of an electronic filing document is established.
[0222] Next, actuation of the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained using drawing 15 .

[0223] First, the electronic contract 41 is read through external storage 114 and a hard disk drive unit 128 to the network 100, and the code data 40 with a header which are authentication data are taken out. Code data 40D is taken out from this code data 40 with a header, it is decrypted by the decryption means 43 using the public key 42 of an external certificate authority, and code data 44D and authentication data 44A are generated. Code data 44D corresponds to code data 36D of drawing 13 , and external authentication data 44A corresponds to external authentication data 36A of drawing 13 .
[0224] Date authentication 44 A-D is taken out from external authentication data 44A. Code data 44D is decrypted by the decryption means 46 using the public key 45 of the contractor second, and code data 47D and authentication data 47A are taken out. Code data 47D corresponds to code data 32D of drawing 13 , and authentication data 47A corresponds to authentication data 32A of the second of drawing 13 .
[0225] Date authentication 47 A-D of the second is taken out from authentication data 47A. Code data 47D is decrypted by the decryption means 49 using the public key 48 of a contractor shell, and description data 50D is taken out.
[0226] The data which removed the authentication data 40 from the electronic filing document 41 on the other hand are equivalent to the data of an electronic filing document 1. The feature-extraction means 51 extracts the description from the data equivalent to an electronic filing document 1, and the description data 52 are obtained.
[0227] Comparison collating of description data 50D and the description data 52 is carried out with the collating means 53, and identity judging 53-J is obtained. If identity judging 53-J shows identitas, the alteration of an electronic filing document is not performed, but the alteration is performed when that is not right.
[0228] Moreover, the external certificate authority to the electronic filing document 1 of first creation and the authentication fact of the second, and an authentication date will be displayed, and the justification about a contract is checked.
[0229] since the external certificate authority to the electronic filing document 1 of the identity judging and the first creation by description data 50 D and 52 and the authentication fact list of the second check an authentication date, the alteration prevention system and the approach of an electronic filing document it start the gestalt of operation of this invention judge the identity of an electronic contract effective, and prove the justification of a document at the place of a trial, so that it mention above.
[0230] In addition, although this operation gestalt explained the case where contractors were two persons of the first and the second, this invention is not restricted in this case. when a contractor turns into three persons of the first, the second, and the third class, even if the step of the second in drawing 15 is attached to the third class, it is carried out repeatedly -- being sufficient . What is necessary is just to carry out by repeating the step of the second, even if attached to ** when a contractor furthermore requires ** further. Therefore, in a contractor's number, the electronic contract exchanged among two or more persons who are not concerned can be checked.
[0231] (Gestalt of the 7th operation) This operation gestalt explains the display edit means at the time of making the electronic filing document 12 with authentication display or print while explaining the concrete example of the edit means of header 11H of drawing 4 or drawing 7 in each above-mentioned operation gestalt, for example.
[0232] Drawing 16 is drawing showing the functional configuration of the alteration prevention system of the electronic filing document of the 7th operation gestalt of this invention, and an example of processing flow, gives the same sign to the same part as drawing 4 , drawing 7 , drawing 9 , drawing 11 , drawing 13 , and drawing 15 , and omits the explanation. The document authentication system 101 shown in drawing 2 or the authentication-text document check system 103 shown in drawing 6 is used for the system of this operation gestalt. The original functional division of this operation gestalt is because correction was added to the document authentication program 133 or the authentication-text document check program 135.

[0233] It comes to add a means to explain below to the document authentication system 101 which shows the alteration prevention system of this electronic filing document to drawing 1 , or the authentication-text document check system 103. In addition, taking the case of the case of the document authentication system 101, it explains hereafter.
[0234] By the document authentication system 101 of this operation gestalt, it has a display printing means besides the same configuration as the 1st, 3rd, and 5th operation gestalt, and the edit means of a header is shown concretely.
[0235] The scanners 115 which incorporate the display object with which seal etc. was pushed as print of a seal 54 which is image information in case header 11H are edited into the edit means of a header (drawing 2 etc.), A means (not shown) to add this print of a seal 54 to some electronic seal 60, and a feature-extraction means 55 to carry out a feature extraction from print of a seal 54, and to generate the description data, An encryption means 58 to encipher the description data 56 with a private key 4, and a means to add the enciphered encryption print of a seal 59 to some electronic seal 60 (not shown), An input means (input unit 112) to add an identifier etc. to the electronic seal 60, and a means (not shown) to add the completed electronic seal 60 to the description data 3 (drawing 16 complex data 11) with a header as header 11H (3H) are established. In addition, the electronic seal 60 comes to compound the identifier of print of a seal 54, the encryption print of a seal 59, and an owner.
[0236] The means which, on the other hand, takes out a date, a signature, and the print-of-a-seal information 61 from header 11H of complex data 11 for a display printing means (not shown), a means 62 to operate these data orthopedically so that it may be settled in a viewing area -- on the other hand -- the electronic filing document 12 with authentication to the electronic filing document 1 -- ** -- with the means (not shown) to take out A means (not shown) to pile up the date, the signature, and print-of-a-seal information orthopedically operated by the tag indicated in the taken-out electronic filing document 1 and viewing-area information 1T, and a means (a display 111, airline printer 113) to print or display this piled-up display document 63 are established.
[0237] Next, actuation of the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained using drawing 16 , drawing 17 , drawing 18 , and drawing 19 .
[0238] Drawing 16 and drawing 17 explain the processing which generates the electronic seal 60 first.
[0239] Drawing 17 is the flow chart showing electronic seal generation processing of the alteration prevention system of the electronic filing document of this operation gestalt.
[0240] First, the owner name of electronic seal is inputted by the input unit 112 (X1). Next, the print-of-a-seal data 54 are read (X2). What print-of-a-seal data read with the scanner 115 what stamped seal on paper, and was electronized is used.
[0241] Next, the description is extracted from the print-of-a-seal data 54 by the feature-extraction means 55, and the description data 56 are generated (X3). It is enciphered by the encryption means 58 with which the description data 56 used an owner's private key 4, and the encryption print of a seal 59 is generated (X4). The owner name inputted at the print-of-a-seal data 54, the encryption print of a seal 59, and step X1 is summarized as one data, and the electronic seal 60 is generated (X5). And it is put into the electronic seal 60 by header data 3H of drawing 1 of the gestalt of the 1st operation. As a result, the data of the electronic seal 60 will be saved header 11H of the electronic filing document 12 with authentication of drawing 16 (X6).
[0242] Next, drawing 18 explains collating processing of the electronic seal which prevented the alteration.
[0243] Drawing 18 is the flow chart showing electronic verification-of-a-seal-impression processing of the alteration prevention system of the electronic filing document of this operation gestalt.
[0244] This collating processing is separately performed with the identity judging of electronic-filing-document 1 the very thing, and evaluates the justification of the electronic seal (electronic signature) contained in header 11H. In addition, although drawing 16 does not show especially the means of this

processing, it realizes by the hardware of the document authentication program 133 or the authentication-text document check program 135, and a system, and that means realizes processing shown by drawing 18 .

[0245] First, an owner name is inputted (Y1). According to an owner name, the owner's public key is read through external storage 114 and a hard disk drive unit 128 to the network 100 (Y2). Next, the encryption print of a seal in the electronic seal 60 is decrypted using a public key (Y3).

[0246] On the other hand, a feature extraction is performed from the print-of-a-seal data in the electronic seal 60 (Y4). Next, collating with the description data decrypted at step Y3 and the description data extracted at step Y4 is performed (Y5).

[0247] The judgment of this collating result is performed (Y6), and that will be displayed by the display 111 if seal is inharmonious. On the other hand, that will be displayed if seal is in agreement.

[0248] Next, drawing 16 and drawing 19 explain the processing which edits a document and a header so that electronic seal and a date may be laid on top of an electronic filing document and it can display or print.

[0249] Drawing 19 is the flow chart showing document header edit processing of the alteration prevention system of the electronic filing document of this operation gestalt.

[0250] First, edit of an electronic filing document 1 is performed (Z1). This processing is the creation activity of electronic-filing-document 1 itself, and is an activity by the system user. Furthermore, a viewing area is set as an electronic filing document 1 by the activity by the system user (Z2). It decides on the location which displays a date, a signature, and print-of-a-seal information in this phase.

[0251] Next, a tag and viewing-area information 1T are embedded at the viewing area created step Z2 inside the electronic filing document 1 (Z3).

[0252] Header edit is started from here and a date, a signature, and the print-of-a-seal information 61 are edited (Z4). The title information furthermore embedded header data 11H is inputted, or the title part in an electronic filing document is specified, and the value is incorporated by header 11H (Z5). And header 11H are saved (Z6).

[0253] Next, an electronic filing document 1 is saved (Z7). In addition, since header 11H the very thing is not necessarily embedded at an electronic filing document 1, document preservation of step X7 may be immediately performed after the tag to the electronic filing document 1 of step Z3, and viewing-area information 1T embedding.

[0254] Since it is recorded by the above processing whether a date, a signature, and the print-of-a-seal information 61 should be displayed in the case of electronic-filing-document 1 throat, when displaying or printing an electronic filing document 1, as drawing 16 showed, on an electronic filing document, a date, a signature, and print of a seal can be piled up, and it can consider as the display document 63 by it.

[0255] The electronic seal 60 which prevented the alteration will be attached to the electronic filing document 12 which prevented the alteration by this, and it will be displayed or printed as a display document 63 on top of which these were laid further.

[0256] As mentioned above, since the alteration prevention system and approach of an electronic filing document concerning the gestalt of operation of this invention added the electronic seal 60 which performed the feature extraction and was enciphered to header 3H, they can judge the existence of a print-of-a-seal alteration of the electronic seal 60, and can stick the print of a seal which prevented the alteration to the electronic filing document.

[0257] Moreover, since it was made to perform display and printing together with the electronic filing document to which an alteration is prevented and the print of a seal which prevented the alteration in this way is made as for the existence judging of an alteration again, the same employment as the document of the conventional paper is attained by the display and printing against which this alteration prevention was secured. Though the same employment as the document of the conventional paper is possible, since a document can be sent to a remote place by transmission in an instant, the effectiveness is very size. In addition, the electronic filing document displayed on the display document

63 in this case is more effective if what performed the identity judging and the authentication check is used.

[0258] In addition, although this operation gestalt explained one electronic seal 60 by the case where it puts into header 3H, this invention is not restricted to this. Since header data can be edited, they can be employed also in use of drawing 13 R> 3 or drawing 15 out of the use in drawing 4 or drawing 7 , and can put in the date, signature and print of a seal of the first, and the date, signature and print of a seal of the second into an electronic filing document. Also in this case, it cannot be overemphasized that electronic-filing-document 1 itself is not altered.

[0259] Furthermore, although [the above explanation] the print of a seal which read with the scanner 115 what stamped seal on paper, and was electronized is used, a handwritten signature may be carried out to paper and the electronic signature read and electronized with the scanner 115 may be used.

[0260] (Gestalt of the 8th operation) this operation gestalt -- above-mentioned the 1- the example of configuration actuation of the feature-extraction means used with the 7th operation gestalt is explained.

[0261] Drawing 20 is drawing for explaining the feature-extraction approach in the alteration prevention system of the electronic filing document of the gestalt of operation of the 8th of this invention.

[0262] Moreover, drawing 21 is drawing showing the functional configuration of the alteration prevention system of the electronic filing document of this operation gestalt, and an example of processing flow, gives the same sign to the same part as drawing 4 , drawing 7 , drawing 9 , drawing 11 , drawing 13 , drawing 15 , and drawing 16 , and omits the explanation. Moreover, the document authentication system 101 shown in drawing 2 or the authentication-text document authentication system 103 shown in drawing 6 is used for the system of this operation gestalt. The original functional division of this operation gestalt is because correction was added to the document authentication program 133 or the authentication-text document check program 135.

[0263] A means to explain below as a feature-extraction means in the document authentication system 101 shown in drawing 1 or the authentication-text document check system 103 is established, and the alteration prevention system of this electronic filing document is constituted. In addition, taking the case of the case of the document authentication system 101, it explains hereafter.

[0264] As shown in drawing 21 , the feature-extraction means 2 (20, 51, 55) of the document authentication system 101 or the authentication-text document check system 103 generates description data 3D from an electronic filing document 1.

[0265] The part which stores data S_sum, 256 arrays which store data IS_sum, and the processing means which is not illustrated are formed in this feature-extraction means 2. This processing means is a functional implementation means to realize processing explained below.

[0266] First, drawing 20 shows the data flow of a feature-extraction means.

[0267] In this drawing, the data, i.e., Stream, itself, such as an electronic filing document and a file, are making electronic-filing-document data list S. This electronic-filing-document data list S is constituted by the electronic-filing-document data list parts S1, S2, S3, .., Sn divided into 256 bytes at a time.

[0268] S_sum_stream generated from this Stream is making sum total data list S_s_stream. This sum total data list S_s_stream consists of sum total data list parts SS1, SS2, and SS3 and .. SS1 -- S1, S2, S3, .., S256 -- let each total value be 256 data lists. the same -- SS2 -- S257-S512 -- each total value is made into the data list.

[0269] On the other hand, from Stream, it is Intervaled. Data list IS which kept spacing as String is generated. Data list IS which kept this spacing consists of data list parts IS1, IS2, IS3, .., ISn which kept spacing. Here, IS1 puts each 256 initial data of S1, S2, S3, .., S256 in order one by one, and IS2 puts the each 2nd 256 data of S1, S2, S3, .., S256 in order one by one. IS3-IS256 are constituted like the following. IS257 puts each 256 initial data of S257-S512 in order one by one. It is the same as that of the following.

[0270] This Intervaled IS_sum_stream generated from String is making sum total data list IS_s_stream which kept spacing. Sum total data list IS_s_stream which kept this spacing consists of the sum total

data list parts ISS1, ISS2, and ISS3 and .. which kept spacing. The sum total data list parts ISS1, ISS2, and ISS3 which kept this spacing, and .. are generated from the data list parts IS1-ISn which kept spacing, and that generation method is the same as the approach of generating SS1, SS2, SS3, and .. from S1-Sn.

[0271] In addition, finally sum total data list S_s_stream and sum total data list IS_s_stream which kept spacing serve as description data 3D.

[0272] Here, it is as follows when the relation between drawing 20 and drawing 21 is explained.

[0273] S1 is 256 bytes of data list, the total value of this data of S1 is stored in S_sum of drawing 21 , and the value of S_sum is outputted to S_s_strem. Even if S_s_strem takes the total value of 256 bytes by the data list of WORD (16 bits), cancellation of significant digits is not generated. Total value is outputted to S_s_steram also to the data list S2 which follows S1 similarly. Hereafter, it is similarly carried out until it results [from S3] in Sn.

[0274] S3 is in IS1 by 256 bytes of data list 1 byte of head of S1, and 1 byte of head of S2, it continues with 1 byte of head, and even 1 byte of head of S256 is stored. IS2 continues by 256 bytes of data list similarly with the 2nd byte of S1, the 2nd byte of S2, and the 2nd byte of S3, and even the 2nd byte of S256 is stored. Similarly, IS3 continues by 256 bytes of data list similarly with the 3rd byte of S1, the 3rd byte of S2, and the 3rd byte of S3, and even the 3rd byte of S256 is stored. 256 continue with the 256th byte of ISS1, the 256th byte of S2, and the 256th byte of S3, and even the 256th byte of S256 is stored. Respectively the sum total is taken, the data from IS1 to IS256 are stored in IS_sum [255] from IS_sum [0] of drawing 21 , and the list of IS_sum is outputted to IS_s_stream. Even if IS_s_stream takes the total value of 256 bytes by the data list of WORD, cancellation of significant digits is not generated.

[0275] In this way, although the description data which consist of S_s_stream and IS_s_stream are obtained, drawing 22 explains the flow of this processing below.

[0276] Drawing 22 is the flow chart showing an example of processing of the alteration prevention system feature data extraction of the electronic filing document of this operation gestalt.

[0277] First, all data are initialized (A1). Next, it is investigated whether there are any data of electronic-filing-document data list S (A2).

[0278] When there are data, it moves to step A3, and 1 byte is read from S. On the other hand, when there are no data, it moves to step A4 and a post process is performed.

[0279] After reading 1 byte from S by step A3, the read value is added to S_sum and IS_sum [i] (A5).

[0280] Next, it is investigated for i whether it is 255 (A6). When i is not 255, 1 **** of i is carried out (A7), and it returns to step A2. On the other hand, when i is 255, the value of (A6) and S_sum is outputted to S_s_stream, and i is returned to zero (A8).

[0281] Next, it is investigated for j whether it is 255 (A9). When j is not 255, 1 **** of j is carried out (A10), and it returns to step A2. On the other hand, when j is 255, the value from (A9) IS_sum[1] to IS_sum [255] is outputted to IS_s_stream, j is returned to zero (A11), and it returns to step 2.

[0282] Every 1 byte of data of an electronic filing document are read one by one, it is continued by generating it the data (S_s_stream, IS_s_stream) of drawing 20 until all data are processed by such processing, and it is outputted as description data 3D.

[0283] When this S_s_stream and IS_s_stream are used as the description data, even if the value of 1 byte of an electronic-filing-document data list S (electronic-filing-document 1 and print-of-a-seal 54 grade) throat changes, 1 word of somewhere in S_s_stream changes. Moreover, even if it replaces 2 bytes of an electronic-filing-document data list S throat, 1 word of somewhere in IS_s_stream changes.

[0284] For example, if data are replaced inside the data-division part of S1, although the total value of S1 does not change, the value of IS_sum [0] to somewhere in IS_sum [255] will surely change. The fact of an alteration is discovered even if it alters the data of electronic-filing-document 1 throat by this. Moreover, since 256 bytes of data of S1 are compressed into 1 word and 256 bytes of data of IS1 are compressed into 1 word, data are compressed into 1/64 of the sizes of the original data. Moreover, on the other hand, compression of data is tropism, and the description data generated in this way cannot

reproduce the original data from the description data.
[0285] As mentioned above, since the alteration prevention system and approach of an electronic filing document concerning the gestalt of operation of this invention generated S_s_stream and IS_s_stream as shown in drawing 20 as description data with the feature-extraction means, however which part of the original data may change, they can discover the change. Moreover, as compared with the original data, data size becomes small sharply, and the description data are easy handling. Moreover, the method of drawing of the description data is simple, and can make an operation a high speed.
[0286] Furthermore, since the original data are unreproducible from the description data, an electronic filing document can be attested with un-indicating for authentication to indicate an electronic filing document 1 to the external certificate authority 99. By the approach using the description data, it is because the turnover of the document itself is unnecessary to authentication of an electronic filing document.
[0287] (Gestalt of the 9th operation) this operation gestalt -- above-mentioned the 1- other examples of configuration actuation of the feature-extraction means used with the 7th operation gestalt are explained.
[0288] Drawing 23 is drawing for explaining the feature-extraction approach in the alteration prevention system of the electronic filing document of the gestalt of operation of the 9th of this invention, gives the same sign to the same part as drawing 20 , and omits the explanation.
[0289] Moreover, the document authentication system 101 shown in the alteration prevention system of the electronic filing document of this operation gestalt at drawing 2 or the authentication-text document authentication system 103 shown in drawing 6 is used, and a means to explain below as a feature-extraction means is established. In addition, the original functional division of this operation gestalt is because correction was added to the document authentication program 133 or the authentication-text document check program 135.
[0290] The feature extraction in this operation gestalt is performed like the 8th operation gestalt until S_s_stream and IS_s_stream are extracted. Moreover, S_s_stream' from S_s_stream and IS_s_stream[from IS_s_stream] ' are generated, and these S_s_stream' and IS_s_stream' are used as final description data 3D. In addition, S_s_stream' and IS_s_stream' consist of long words (32 bits).
[0291] As concrete processing, it is as follows.
[0292] First, it is the same as that of the 8th operation gestalt up to this side which generates SS1 grade and ISS1 grade. With the gestalt of the 8th operation, it was outputting as it is as S_s_stream and IS_s_stream, without dividing SS1 grade and ISS1 grade by 256 word units in actual processing. On the other hand, it is the train of the value which totals S1, S2, S3, .., every 256 bytes of Sn, and changes in drawing 23 every 256 words SS1 and SS2 -- It is made the train of the long word of the total value of SS256, and outputs to S_s_stream'. Moreover, the train of the long word of the total value of IS1, IS2, IS3, .., IS256 is outputted to IS_s_stream'.
[0293] if it puts in another way -- S_s_stream' -- SS1, SS2, and .. each total value outputs as a data list one by one -- having -- the same -- IS_s_stream' -- ISS1, ISS2, and .. each total value is outputted as a data list one by one.
[0294] By this, although S_s_stream was the stream of WORD in drawing 20 , S_s_stream' becomes the stream of a long word by drawing 23 . Similarly, although IS_s_stream was the stream of WORD in drawing 20 , IS_s_stream serves as a stream of a long word in drawing 23 . thereby -- the amount of data -- further -- it is compressed into 1/128 and becomes 1/8192 of the magnitude of the beginning.
[0295] As mentioned above, since the feature-extraction means generated S_s_stream' and IS_s_stream' as shown in drawing 23 as description data, the same effectiveness as the 8th operation gestalt is acquired, and also the alteration prevention system and approach of an electronic filing document concerning the gestalt of operation of this invention can make the description data compact more nearly further than the case where it is the 8th operation gestalt.
[0296] In addition, although every 256 of data are totaled once in the excess to the 8th operation

gestalt with the 9th operation gestalt, only at once, there is nothing and data may be compressed further repeatedly. If it does in this way, the description data can be further made compact.
[0297] (Gestalt of the 10th operation) this operation gestalt -- above-mentioned the 1- the example of further others of configuration actuation of the feature-extraction means used with the 7th operation gestalt is explained.
[0298] Drawing 24 is drawing for explaining the feature-extraction approach in the alteration prevention system of the electronic filing document of the gestalt of operation of the 10th of this invention.
[0299] Moreover, drawing 25 is drawing showing the functional configuration of the alteration prevention system of the electronic filing document of this operation gestalt, and an example of processing flow, gives the same sign to the same part as drawing 4 , drawing 7 , drawing 9 , drawing 11 , drawing 13 , drawing 15 , and drawing 16 , and omits the explanation. Moreover, the document authentication system 101 shown in drawing 2 or the authentication-text document authentication system 103 shown in drawing 6 is used for the system of this operation gestalt. The original functional division of this operation gestalt is because correction was added to the document authentication program 133 or the authentication-text document check program 135.
[0300] A means to explain below as a feature-extraction means in the document authentication system 101 shown in drawing 1 or the authentication-text document check system 103 is established, and the alteration prevention system of this electronic filing document is constituted. In addition, taking the case of the case of the document authentication system 101, it explains hereafter.
[0301] As shown in drawing 25 , the feature-extraction means 2 (20, 51, 55) of the document authentication system 101 or the authentication-text document check system 103 generates description data 3D from an electronic filing document 1.
[0302] Separator table 2T and word array 2W are prepared in the feature-extraction means 2.
[0303] On the other hand, in drawing 24 , an electronic filing document 1 consists of lists of a word and a separator. A separator separates words, such as a null and punctuation, into a document. Word array 2W consist of the data lists and sequence of a word. On the other hand, description data 3D consists of sequence data lists of the data list of word array 2W.
[0304] Moreover, separator table 2T register what is beforehand used as a separator. On the other hand, word array 2W consist of sequence of the field which stores a word, and an array.
[0305] Next, the feature-extraction processing in the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained.
[0306] First, as drawing 24 shows, it is considered that the data which data read from the head of the electronic filing document 1 which consisted of a word and a separator one by one, and were divided with rareness, the separator, and the separator are a word. A new thing is registered into word array 2W among the found words, and the array number of the word is written out to description data 3D. That is, the list of this array number itself serves as the description data.
[0307] That is, it is compared with the data whose one character read by the feature-extraction means 2 is separator table 2T, and if it is not a separator, the following one character will be read. Read in is performed one by one and the character string which continued reading and was obtained is detected as a word. In this case, it is judged whether the character string concerned is a new word. And in the case of a new word, it registers character-array 2W, and a registration number is written out as description data 3D. In the case of the word which already came out, the registration number is written out at description data 3D.
[0308] This processing is more concretely explained using drawing 26 .
[0309] Drawing 26 is the flow chart showing an example of processing of the alteration prevention system feature data extraction of the electronic filing document of this operation gestalt.
[0310] First, all data are initialized (B1). Next, one character is read, when it is investigated whether there are any data of an electronic filing document 1 and there are (B-2) and data (B3). When there are

no data, the (B-2) post process is performed (B4).
[0311] Next, one read character is performed by the comparison with the data whether whose it is a separator it is separator table 2T (B5). When one read character is a separator, the comparison of (B5) separator table 2T and a separator is performed (B6). On the other hand, when one read character is not a separator, (B5) and its alphabetic character are put into a buffer, and it returns to step B-2 (B7).
[0312] The comparison of the table data (hash table) of array 2W and buffer data is performed after step B6 (B8). In addition, step B6 determines the class of the separator itself and step B8 determines the class of word constituted in the buffer.
[0313] Next, when a separator is not the same as table data (array 2W) than the result of step B6, (B9) and data are registered into table 2W (B10), and move to step B11. On the other hand, in being the same, it moves to step B11, without performing (B9) and step B10.
[0314] At step B11, when buffer data are not the same as table data (array 2W), buffer data are registered into hash table 2W (B12), and move to step B13. On the other hand, in being the same (B11), it moves to step B13, without performing step B12.
[0315] And at step B13, the table number of a separator and each word determined as description data 3D at steps B9-B12 is outputted. It returns to step B-2 after that.
[0316] The description of an electronic filing document 1 is extracted by the above as a table number list of a hash table, and it is obtained as description data 3D.
[0317] As mentioned above, since the alteration prevention system and approach of an electronic filing document concerning the gestalt of operation of this invention extracted the list of the table number of a word and a separator as description data with the feature-extraction means, however which part of the original data may change, they can discover the change. Moreover, as compared with the original data, the size of data becomes small sharply, and handling is easy. Since the original data are furthermore unreproducible from the description data, even if it is the case where he does not want to indicate an electronic filing document to an external certificate authority, an electronic filing document can be attested.
[0318] (Gestalt of the 11th operation) this operation gestalt -- the 1- in using each document authentication system 101 in the alteration prevention system of an electronic filing document explained with the 7th operation gestalt, the external authentication system 102, and the authentication-text document check system 103, a means to generate the cryptographic keys (a private key, public key, etc.) which generate the information for checking the system user, and are used by each system is explained.
[0319] Drawing 27 is drawing showing the functional configuration of the 11th of the alteration prevention system of the electronic filing document of the gestalt of operation of this invention, and an example of processing flow, gives the same sign to the same part as drawing 4 , drawing 7 , drawing 9 , drawing 11 , drawing 13 R> 3, drawing 15 , and drawing 16 , and omits the explanation. Moreover, the authentication-text document authentication system 103 shown in the document authentication system 101 shown in drawing 2 , the external authentication system 102 shown in drawing 3 , or drawing 6 is used for the system of this operation gestalt. The original functional division of this operation gestalt is because correction was added to the document authentication program 133, the external authentication program 134, or the authentication-text document check program 135.
[0320] Below, each means is added and the alteration prevention system of this electronic filing document is constituted by the same configuration as the document authentication system 101, the external authentication system 102, or the authentication-text document check system 103 shown in drawing 1 . In addition, taking the case of the case of the document authentication system 101, it explains hereafter.
[0321] It generates the he authentication data 78 further from a user name, ID (identification information), a password, a fingerprint, the generated cryptographic key while the document authentication system 101 shown in drawing 27 reads a system user's fingerprint, performs a feature

extraction and generates cryptographic keys 71, 74, 75, 77S, and 77K using this description data 67, the password 68 entered separately, and a random number. This he authentication data 78 is used for checking a system user in the 12th operation gestalt mentioned later.

[0322] In order to generate this he authentication data 78 to the document authentication system 101 The fingerprint reader 64 and a feature-extraction means 66 to extract the description data 67 from the fingerprint 65 read as an image data, A cryptographic key generation means 70 to generate a cryptographic key 71 from a password 68 and the description data 67 among the password 68 entered from the input unit 112, and a name and ID69, A private key public key generation means 73 to generate a private key 74 and a public key from the random number generated from a random number generator 72 and a random number generator 72, a password 68, and the description data 67, An encryption means to generate encryption private key 77S and encryption cryptographic key 77K from a cryptographic key 71 and a private key 74 is established. furthermore -- the document authentication system 101 -- a fingerprint 65, encryption private key 77S, and the encryption cryptographic key 77 -- him who incorporates K, a password 68, and a name and ID69, and consists of fingerprint 78F, encryption private key 78S, encryption cryptographic key 78K, password 78P, and a name and ID78N -- a means (not shown) to create the authentication data 78 is established.

[0323] Next, actuation of the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained using drawing 27 and drawing 28 .

[0324] Drawing 28 is the flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.

[0325] him [in / in this actuation / the time of the system startup of the document authentication system 101 etc.] -- it is the procedure which creates the data for authentication.

[0326] For this reason, first, a name and the ID data 69, and a password 68 are first entered by the input device 112, and a system is started (C1). Next, the fingerprint reader 64 is started and a fingerprint is read (C2). Thereby, the fingerprint data 65 are obtained.

[0327] Next, the description data 67 are extracted from the fingerprint data 65 by the feature-extraction means 66 (C3). Furthermore a password 68 and the description data 67 are used, and a cryptographic key 71 is generated by the cryptographic key generation means 70 (C4).

[0328] Next, a password 68, a random number generator 72, and the description data 67 are used, and a private key 74 and a public key 75 are generated by the private key public key generation means 73 (C4). With this operation gestalt, the thing corresponding to a RSA method is used as a private key public key generation means 73. In addition, DES etc. may be used.

[0329] Next, a cryptographic key 71 and a private key 74 are enciphered by the encryption means 76, and encryption private key 77S and encryption cryptographic key 77K are generated (C6). In addition, with this operation gestalt, the encryption means 76 uses the DES method which is one of the common key encryption systems, and makes the cryptographic key 71 the cryptographic key. About a cryptographic key 71, it is enciphering oneself by oneself (generation of encryption cryptographic key 77K).

[0330] and the fingerprint data 65, encryption private key 77S, encryption cryptographic key 77K, a password 68, and a name and ID69 -- him -- it is collected into one as authentication data 78 (C7), and is stored in hard disk drive unit 128 grade (C8). Moreover, a public key 75 will be registered into a predetermined location among this information (C9).

[0331] since the alteration prevention system and approach of an electronic filing document concerning the gestalt of operation of this invention are carried out based on fingerprint data and generated the cryptographic key, as mentioned above -- him -- while being able to make authentication into a positive thing, he does not need to know the data of a cryptographic key itself and can make use of a system simple. moreover -- from [that the cryptographic key itself is enciphered and that the private key is enciphered] -- even if -- him -- even if the authentication data 78 are sometimes stolen, the contents

of a cryptographic key and the private key cannot be known, but very safe information management can be performed.
[0332] In addition, in such a case, this invention is not restricted although the password was needed for the cryptographic key generation means 70 with this operation gestalt. For example, even if it generates a cryptographic key only from the description data 67, the same effectiveness can obtain. Moreover, although the password 68 and the random number generator 72 were needed, for example for the private key public key generation means 73, the same effectiveness is able to obtain, whether there is no either or there are no both.
[0333] Furthermore, although [this operation gestalt] a fingerprint is used for generation of a cryptographic key etc., this invention can use various living body data, if it is not restricted to a fingerprint and a voiceprint, the iris, etc. can specify him.
[0334] (Gestalt of the 12th operation) This operation gestalt enables it to use the system concerned for the system user who registered by the system of the 11th operation gestalt. namely, the 1- in using each document authentication system 101 in the alteration prevention system of an electronic filing document explained with the 7th operation gestalt, the external authentication system 102, and the authentication-text document check system 103, the means which makes usable the cryptographic keys (a private key, public key, etc.) which check the system user and are used by each system is explained.
[0335] Drawing 29 is drawing showing the functional configuration of the 12th of the alteration prevention system of the electronic filing document of the gestalt of operation of this invention, and an example of processing flow, gives the same sign to the same part as drawing 4 , drawing 7 , drawing 9 , drawing 11 , drawing 13 R> 3, drawing 15 , drawing 16 , and drawing 27 , and omits the explanation. Moreover, the authentication-text document authentication system 103 shown in the document authentication system 101 shown in drawing 2 , the external authentication system 102 shown in drawing 3 , or drawing 6 is used for the system of this operation gestalt. The original functional division of this operation gestalt is because correction was added to the document authentication program 133, the external authentication program 134, or the authentication-text document check program 135.
[0336] Below, each means is added and the alteration prevention system of this electronic filing document is constituted by the same configuration as the document authentication system 101, the external authentication system 102, or the authentication-text document check system 103 shown in drawing 1 . In addition, taking the case of the case of the document authentication system 101, it explains hereafter.
[0337] When those who have just use authority want to use the alteration prevention system of an electronic filing document, the document authentication system 101 shown in drawing 29 him who was made to input a password 68 and a fingerprint 65, and was generated with this and the 11th operation gestalt -- fingerprint 78F beforehand stored in the authentication data 78 -- Decode encryption private key 78S by this cryptographic key further, and a private key 4 is taken out. password 78P -- him -- fingerprint 78F after checking, password 78P, and encryption cryptographic key 78K to a cryptographic key -- drawing -- the 1- the alteration prevention system of the electronic filing document of the 7th operation gestalt is changed into an usable condition.
[0338] for this reason, the fingerprint 65 read with the fingerprint reader 64 by the document authentication system 101 and him -- a collating means 81 to collate fingerprint 78F in the authentication data 78, the password 68 entered from the input device 112, and him -- a collating means 80 to collate password 78P in the authentication data 78, and a judgment logic means 82 to judge he authentication from the result of the collating means 80 and 81 are established. Furthermore, a feature-extraction means 66 to extract the description data 67 from fingerprint 78F if the purport with which he was attested is received in the document authentication system 101 from the judgment logic means 82, A cryptographic key generation means 70 to generate a cryptographic key 71 from the description data 67 and password 78P, The decode means 83 which decodes encryption cryptographic key 78K by the cryptographic key 71, and takes out a cryptographic key 84, A collating means 85 to

check that the cryptographic key 71 and the cryptographic key 84 were collated, and the cryptographic key 71 has been taken out correctly, The decode means 86 which takes out the private key 4 used by the alteration prevention systems (drawing 4 etc.) of an electronic filing document from the encryption private key 78 using the taken-out cryptographic key 71, and a display means 79 to display a name, ID78N, etc. are established.

[0339] Next, actuation of the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained using drawing 29 and drawing 30 .

[0340] Drawing 30 is the flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.

[0341] this actuation -- the input of living body data etc. -- him -- him [in / the time of the system startup of the document authentication system 101 etc. / based on the data for authentication] -- it is the procedure which performs check and private key generation.

[0342] First, if an identifier is inputted in order to perform he authentication from an input device 112, the he authentication data 78 will be read from a hard disk drive unit 128, and a name and ID will be displayed by the display means 111. A system user checks a name and ID and enters a password 68 (D1).

[0343] next, him -- the password 68 entered password 78P and now in the authentication data 78 is collated (D2). If this collating is in agreement, a fingerprint will be read with the fingerprint reader 64, and the fingerprint 65 which is an image data is generated (D3).

[0344] Next, fingerprint 78F and the read fingerprint 65 are collated by the fingerprint authentication means 81 (D4). if collating is in agreement (D4) -- him -- fingerprint 78F are taken out from the authentication data 78, a feature extraction is carried out by the feature-extraction means 66, and the description data 67 are generated (D5). the ** which does not use the fingerprint 65 read here -- him -- it is for producing some difference, whenever it is not possible and takes more that the fingerprint 65 which using fingerprint 78F in the authentication data 78 read is in agreement with fingerprint 78F, without 1 bit being different. on the other hand -- a feature extraction -- the 8- since it is extracted as description data which are different even if there is a slight difference, as the 10th operation gestalt explained, it is going to take out a cryptographic key 71 using the fingerprint itself taken out with the 11th operation gestalt.

[0345] That is, this description data 67 and password 78P are used, and a cryptographic key 71 is generated by the cryptographic key generation means 70 (D6). Next, the cryptographic key 71 which encryption cryptographic key 78K were taken out from the he authentication data 78, and was generated at step D6 decodes (D7).

[0346] The cryptographic key 84 furthermore decoded at a step ST 7 and the cryptographic key 71 generated at a step ST 6 are collated with the collating means 85 (D8). If collating is in agreement, it will be considered that his authentication was finally completed. and him -- encryption private key 78S are taken out from the authentication data 78, it decodes with the decode means 86 using a cryptographic key 71, and a private key 4 is generated (D9).

[0347] In this way, the alteration prevention system of an electronic filing document becomes usable, and processing explained with each operation gestalten, such as document read (D10), a feature extraction (D11), and the description data encryption (D12) by the private key 4, will be performed.

[0348] the alteration prevention system and approach of an electronic filing document which start the gestalt of operation of this invention as mentioned above -- a system user's fingerprint 65 -- reading -- this and him -- since the authentication data 78 were collated -- him -- a private key 4 can be picked out from the authentication data 78. here -- him -- since the private key and the cryptographic key are enciphered and saved in the authentication data 78 -- temporary -- him -- even if authentication data are stolen, a private key and a cryptographic key cannot be known but it is very safe. moreover, a cryptographic key -- him -- since it is generated from fingerprint 78F saved in authentication data,

while the certainly same code data are reproducible, there is no need of telling whom about the code data itself, and it is very safe.
[0349] In addition, although the password was also used for the cryptographic key generation means 70 with this operation gestalt, it is made to correspond to the modification in the 11th operation gestalt, and you may make it only the description data 67 generate a cryptographic key. although it was dealt with with this operation gestalt about the key enciphered using the fingerprint, if this invention is what is not restricted to a fingerprint and can specify him, such as a voiceprint and the iris, -- various living body data -- using -- him -- it may be made to attest.
[0350] (Gestalt of the 13th operation) This operation gestalt explains a means to generate a fingerprint 65 from the information read with the fingerprint reader 64 in the system of the 11th and 12th operation gestalten, and a feature-extraction means 66 to perform a feature extraction from a fingerprint 65.
[0351] Drawing 31 is drawing showing the functional configuration of the 13th of the alteration prevention system of the electronic filing document of the gestalt of operation of this invention, and an example of processing flow, gives the same sign to the same part as drawing 4 , drawing 7 , drawing 9 , drawing 11 , drawing 13 R> 3, drawing 15 , drawing 16 , drawing 27 , and drawing 29 , and omits the explanation. Moreover, the authentication-text document authentication system 103 shown in the document authentication system 101 shown in drawing 2 , the external authentication system 102 shown in drawing 3 , or drawing 6 is used for the system of this operation gestalt. The original functional division of this operation gestalt is because correction was added to the document authentication program 133, the external authentication program 134, or the authentication-text document check program 135.
[0352] Below, each means is added and the alteration prevention system of this electronic filing document is constituted by the same configuration as the document authentication system 101, the external authentication system 102, or the authentication-text document check system 103 shown in drawing 1 . In addition, taking the case of the case of the document authentication system 101, it explains hereafter.
[0353] The document authentication system 101 shown in drawing 31 is constituted by a fingerprint data extraction means 87 to generate a fingerprint 65 from fingerprint Hara data 87F from the fingerprint reader 64, and feature-extraction means 66 to extract the description data 67 from a fingerprint 65.
[0354] Boundary extract means 87A, embossing means 87E, profile extract means 87L, and binary-ized means 87B are prepared in the fingerprint data extraction means 87.
[0355] On the other hand, matching means 66M which make field logging means 66S which start data 66SD from a fingerprint 65, and started data 66SD and pattern 66P prepared beforehand match, and a means (not shown) generated by matching means 66M to generate the description data 67 from data 66D by the single figure are formed in the feature-extraction means 66.
[0356] Next, actuation of the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained using drawing 31 , drawing 32 , drawing 33 , drawing 34 , and drawing 35 .
[0357] Drawing 32 is drawing showing an example of the fingerprint data 65.
[0358] Drawing 33 is drawing showing an example of data 66SD started from the fingerprint data 65 to the rectangle field.
[0359] Drawing 34 is drawing having shown a part of example of the pattern made to match.
[0360] Drawing 35 is the flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[0361] In drawing 35 , first, the data about a fingerprint are read by the fingerprint reader 64, and fingerprint Hara data 87F are obtained (E1).
[0362] Next, embossing of the data which the boundary of fingerprint data was clarified by boundary extract means 87A (E2), and clarified the boundary by embossing means 87E further is taken (E3). Next, the profile extract of data is performed (E4), extract data are further made binary, and the fingerprint

data 65 are obtained (E5). The sample of the fingerprint data 65 which carried out in this way and were obtained to drawing 32 is shown.
[0363] Next, logging of data 66SD is performed, a field being specified by field logging means 66S (E6). Thus, the sample of the cut-down data is shown in drawing 33 .
[0364] Next, pattern matching of data 66SD and pattern data 66P is performed by matching means 66M (drawing 35 E7). An example of the pattern which matches with drawing 34 is shown. If pattern match CHINGU is materialized, matching data will be taken out from matching means 66M, and this will be set to single figure data 66D (E8).
[0365] Next, it is investigated whether the digit count required to generate the description data was read from the fingerprint 65, and when there are still data, steps E6-E8 are repeated (E9). If it finishes reading a required digit count (E9), the description data 67 generated from single figure data 66D will be outputted.
[0366] Generation of the description data 67 for the above to generate a cryptographic key from the fingerprint data 65 is performed.
[0367] him [in / for this / the 11th and 12th operation gestalten] since the alteration prevention system and approach of an electronic filing document concerning the gestalt of operation of this invention can generate the description data 67 for generating a cryptographic key from the fingerprint data 65 as mentioned above -- it can use for authentication and a private key decode system, and the effectiveness is very large.
[0368] [-- the 14- explanation] about the 17th operation gestalt -- above-mentioned the 1- him who did document preparation according to invention explained to the 13th operation gestalt -- the document alteration by him who created can also be prevented by adding authentication of an external certificate authority to except, and it becomes possible to electronize an important document.
[0369] However, when another author adds a partial change to the drawn-up document and it is made a new document, the author, the original new author, and an original external certificate authority need to attest again.
[0370] Then, in the following operation gestalten [14-17th], when an electronic filing document is changed by modification persons other than the original author about modification of the electronic filing document and data which attested for alteration prevention, the approach and system which make possible the reconfirmation certificate of a modification electronic filing document are explained, maintaining authentication of the original author concerned. That is, with the following operation gestalten, it is dealt with while giving credibility, clarifying modification hysteresis of the electronic filing document which two or more authors drew up over two or more stages, and a sex is raised, and electronization of modification documents, such as a hysteresis document conventionally made only in paper, is realized.
[0371] drawing 36 -- the 14- of this invention -- it is drawing showing the overall configuration of the alteration prevention system of an electronic filing document including document modification in the 17th operation gestalt, and an approach.
[0372] As shown in this drawing, the network 1100 using a public line or a dedicated line is constituted, and the document authentication system 1101, the external authentication system 1102 of the external certificate authority 1099, the document modification authentication system 1103, and the authentication-text document check system 1104 are connected to the network concerned.
[0373] the document authentication system 1101 -- the 1- they are the document authentication system 101 explained with the 13th operation gestalt, and the system constituted similarly. The external authentication system 1102 receives the information which should be attested from the document authentication system 1101, and answers a letter in the attested result. Moreover, through a network 1100, the external authentication system 1102 receives the information which should be attested from the document modification authentication system 1103, and answers a letter in the attested result.
[0374] Two or more document authentication systems 1101, document modification authentication

systems 1103, and authentication-text document check systems 1104 may exist, and are used by different user.

[0375] Moreover, the document authentication system 1101, the external authentication system 1102, the document modification authentication system 1103, and the authentication-text document check system 1104 add a display, an input unit or a fingerprint reader, scanner equipment, etc. to computers, such as a workstation and a personal computer, and each function which is different because programs of operation differ fundamentally is realized. Therefore, the document authentication system 1101, the document modification authentication system 1103, and the authentication-text document check system 1104 may be constituted on one computer.

[0376] Furthermore, it is made to constitute on the computer to which the document modification authentication system 1103 and the external authentication system 1102 are connected by the same computer or LAN, and it is also possible in an external certificate authority for it to be made to perform all the authentications.

[0377] The modification authentication system and approach of an electronic filing document in connection with this invention combine suitably these document authentication systems 1101, the external authentication system 1102, the document modification authentication system 1103, and the authentication-text document check system 1104, or are the thing which changes in part, combining a function suitably. further -- this specification -- for convenience -- the 1- the 13th operation gestalt and the 14- each system which belongs to both the operation gestalt group although it divides into the 17th operation gestalt and being explained -- suitably -- combining -- or the part -- it is also possible to combine a function suitably and to incorporate it again.

[0378] Moreover, although the case where it is premised on an instant transfer of the information through a network in the above-mentioned case is explained, it is also possible to exchange required information through the record media 97 and 98, such as a floppy disk, between the document modification authentication system 1103 - the authentication-text document check system 1104 between the document modification authentication system 1101 - the external authentication system 1102 or between the document authentication system 1101 - the document modification authentication system 1103, as shown in drawing 36 R> 6.

[0379] the 14- which corresponds about the alteration prevention system and approach including document modification which has the above system configuration on the whole of an electronic filing document -- the 17th operation gestalt is explained.

[0380] (Gestalt of the 14th operation) This operation gestalt is related with the modification system and approach of an electronic filing document that an alteration can be prevented.

[0381] Drawing 37 is the block diagram showing the example of a hardware configuration of the document modification authentication system applied to the alteration prevention system of an electronic filing document including document modification concerning the 14th operation gestalt of this invention.

[0382] As for the document modification authentication system 1103, it has come to connect a display 1111, an input unit 1112, an airline printer 1113, external storage 1114, the fingerprint reader 1064, and a scanner 1115 with a computer 1110.

[0383] The above-mentioned hardware configuration of this document modification authentication system 1103 is the same as that of the document authentication system 101 shown in drawing 2 , and omits explanation here. That is, a computer 1110, a display 1111, an input unit 1112, an airline printer 1113, external storage 1114, the fingerprint reader 1064, and a scanner 1115 are equivalent to a computer 110, a display 111, an input unit 112, an airline printer 113, external storage 114, the fingerprint reader 64, and a scanner 115, respectively.

[0384] Moreover, the same is said of the configuration in a computer 1110, and each components 1116-1133 of the document modification authentication system 1103 are equivalent to each components 116-133 of the document authentication system 101.

[0385] However, the part corresponding to the document modification authentication system 1103 will become original with this operation gestalt among the software-based elements stored in a hard disk drive unit 1128 or RAM1119 grade. That is, the program storing section 1130 stores the program which realizes the document modification authentication system 1101, and RAM1119 stores the document modification authentication program 1133. In addition, like the 1st operation gestalt, this document modification authentication program 1133 is called from the program storing section 1130 of a hard disk drive unit 1128, and is stored in RAM1119.
[0386] Moreover, CPU1117 controls each part according to the document modification authentication program 1133 in RAM1119, and realizes the document modification authentication system 1103.
[0387] Each means (each processing) or each means (each processing) which is not illustrated expressed by a processing explanatory view, a flow chart, etc. in this operation gestalt and each following operation gestalt is a functional implementation means by actuation of CPU1117 which mainly follows the document modification authentication program 1133.
[0388] Next, the hardware configuration of an external authentication system is explained.
[0389] Drawing 38 is the block diagram showing the example of a hardware configuration of the external authentication system applied to the alteration prevention system of an electronic filing document including document modification of this operation gestalt, gives the same sign to the same part as drawing 37 R> 7, and omits the explanation.
[0390] The external authentication system 1102 consists of the same computing systems as the document modification authentication system 1103. The difference with the document modification authentication system 1103 is a program of operation stored in the program storing section of a hard disk drive unit 1128. This program of operation is called and it is stored as an external authentication program 1134 in RAM1119. CPU1117 controls each part according to this external authentication program, and the external authentication system 1102 is realized. Moreover, the point that a software resource (especially external authentication program 1134) and hardware resources join together, and a functional implementation means is constituted is the same as that of the case of the document modification authentication system 1103.
[0391] Next, each configuration of the alteration prevention system of the electronic filing document which included document modification using drawing 39 and drawing 40 is explained.
[0392] Drawing 39 and drawing 40 are drawings showing the functional configuration of the alteration prevention system of an electronic filing document including document modification of this operation gestalt, and an example of processing flow.
[0393] The alteration prevention system of an electronic filing document including this document modification consists of a document modification authentication system 1103 and an external authentication system 1102.
[0394] The configuration of drawing 39 is explained first.
[0395] The document modification authentication system 1103 consists of a separation means 1005, modification and the authentication means 1006 of modification person #n, and a coupling means 1009, and generates the electronic filing document 1011 with modification hysteresis from the electronic filing document 1001 with modification hysteresis.
[0396] Although there is no modification in the electronic filing document or the past which had modification in the past, the electronic filing document 1001 with modification hysteresis is an electronic filing document which will change from now on, and consists of a original electronic filing document 1002 with authentication, modification part data 1003 with authentication from the 1st modification to the n-1st modification, and the n-1st modification electronic filing documents 1004 with authentication here.
[0397] The separation means 1005 divides the electronic filing document 1001 with modification hysteresis into each component.
[0398] Modification and the authentication means 1006 of modification person #n are the n-th modification part 1007 send out the n-1st modification electronic filing documents 1004 with

authentication to the external authentication system 102, and according to modification person #n based on the response result, and modification person #n. The n-th modification electronic filing document 1008 to depend is outputted.

[0399] A coupling means 1009 is [the original electronic filing document 1002 with authentication, the modification part data 1003 with authentication from the 1st modification to the n-1st modification, and] modification person #n. The n-th modification part 1007 to depend and modification person #n The n-th modification electronic filing document 1008 to depend is combined, and the electronic filing document 1011 with modification hysteresis is generated. Here, the electronic filing document 1011 with modification hysteresis consists of a original electronic filing document 1002 with authentication, a modification part 1010 from the 1st time to the n-th time, and a n-th modification electronic filing document 1008.

[0400] Next, modification of modification person #n, the detail configuration of the authentication means 1006, and the outline configuration of the external authentication system 1102 are explained using drawing 40 .

[0401] modification and the authentication means 1006 of modification person #n -- the document modification means 1021 and difference -- it has the extract means 1023, the modification person authentication means 1025A and 1025B, and a coupling means 1028.

[0402] The document modification means 1021 transforms the modification electronic filing document 1020 into the modification electronic filing document 1022 by modification person #n. difference -- difference with the modification electronic filing document 1022 according [the extract means 1023] to the modification electronic filing document 1020 and modification person #n -- extracting -- this difference -- the n-th modification part 1024 which consists of data is generated.

[0403] the modification person authentication means 1025A and 1025B -- respectively -- a modification person's authentication data -- the modification electronic filing document 1022 and the modification part 1024 -- attesting -- modification person authentication data 1026A and a modification person -- difference -- authentication data 1026B is outputted.

[0404] A coupling means 1028 combines the authentication data 1027 and modification person authentication data 1026A, and outputs the joint authentication data 1029.

[0405] Although not illustrated especially, modification and the authentication means 1006 of modification person #n have a means combines further the means which takes out the modification electronic filing document 1020 and the authentication data 1027 from the n-1st modification electronic filing documents 1004 with authentication, a means combine the modification part 1024 and authentication data 1032B, and generate the modification part 1007, and the modification electronic filing document 1022 and authentication data 1032A, and generate the modification electronic filing document 8.

[0406] external authentication means 1030A which the external authentication system 102 performs authentication by the external certificate authority to the authentication data 1029, and, on the other hand, generates authentication data 1031A, and a modification person -- difference -- it has external authentication means 1030B which performs authentication by the external certificate authority and generates authentication data 1031B to authentication data 1026B.

[0407] in addition, the authentication data 1029 and a modification person -- difference -- authentication data 1026B is transmitted to the external authentication system 1102 from the document modification authentication system 1103, and the authentication results 1031A and 1031B are answered from the external authentication system 1102.

[0408] Next, modification person authentication means 1025A of modification of modification person #n and the authentication means 1006 is explained using drawing 41 .

[0409] Drawing 41 is drawing showing modification of modification person #n, and the configuration of the modification person authentication means in an authentication means.

[0410] Modification authentication means 1025A is equipped with feature-extraction means 1025A-1

and encryption means 1025A-4 while it holds private key 1025A-3 and header 1026 A-H of modification person #n.
[0411] Feature-extraction means 1025A-1 extracts description data 1025A-2 from the modification electronic filing document 22, and it hands them over to encryption means 1025A-4. Encryption means 1025A-4 encipher description data 1025A-2 by private key 1025A-3 of modification person #n, and they generate code data 1026 A-D.
[0412] Modification authentication means 1025A adds header 1026 A-H to code data 1026 A-D, and generates a modification person's authentication data 1026A.
[0413] In addition, although not illustrated especially about modification person authentication means 1025B, it is constituted like modification person authentication means 1025A.
[0414] Drawing 42 is drawing showing the configuration of the external authentication means in an external authentication system.
[0415] External authentication means 1030A is equipped with coupling means 1030A and encryption means 1030A-3 while it holds private key 1030A-2 of external authentication data 1030 A-A including the authentication activation ID, and an external certificate authority.
[0416] The joint authentication data 1029 transmitted from the document modification authentication system 1103 consist of authentication data 1026A of the modification person who consists of header 1026 A-H and code data 1026 A-D, and authentication data 1027. This joint authentication data 1029 is divided into header 1031 A-H, and code data 1026 A-D and the authentication data 1027 in external authentication means 1030A.
[0417] Encryption means 1030A combines external authentication data 1030 A-A, and code data 1026 A-D and the authentication data 1027, and encryption means 1030A-3 encipher this joint result by private key 1030A-2.
[0418] Authentication data 1031A of an external certificate authority finally generated by external authentication means 1030A consists of code data 1031 A-D enciphered as header 1031 A-H by encryption means 1030A-3.
[0419] In addition, although especially external authentication means 1030B is not illustrated and explained, this is the same as what read A and B in external authentication means 1030A.
[0420] Next, actuation of the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained using drawing 39 - drawing 43 .
[0421] Drawing 43 is the flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[0422] First, in the document modification authentication system 1103, reading of the electronic filing document 1001 with modification hysteresis is performed (SS1).
[0423] next, the separation means 1005 -- the original electronic filing document 1002 with modification hysteresis, and with modification hysteresis -- the modification part 1003 to the n-1st time, and with modification hysteresis -- it separates into the n-1st modification electronic filing documents 1004 (SS2).
[0424] Processing from the following step SS 3 to SS7 is performed by modification and the authentication means 1006. That is, as shown in drawing 39 and drawing 40 , it is modification person #n (to the configuration of the same kind and the data which may exist, hereafter). a case -- #1, #2, .., or the 1st .. [2nd] -- describing -- distinguishing -- with modification and the authentication means 6 of using it The n-1st taken-out modification electronic filing documents 1004 with authentication are changed, and authentication of modification person #n is performed, and the authentication data of modification person #n are transmitted to the external authentication system 1102.
[0425] Specifically, the n-1st modification electronic filing document 1020 is first taken out from the n-1st modification electronic filing documents 1004 with authentication. Further. By the alter operation of modification person #n, by the modification means 1021, the n-1st modification electronic filing

documents 1020 are changed, and the modification electronic filing document 1022 which is the n-th time is generated (SS3).
[0426] next, difference -- the extract of the n-1st modification electronic filing documents 1020, the n-th modification electronic filing document 1022, and difference carries out with the extract means 1023 -- having -- the difference of the n-th modification part 1024 -- data are extracted (SS4, drawing 40).
[0427] This processing (SS4) is made like next, and is made. That is, each electronic filing document is binary data which consist of places 0 and 1 got blocked. difference -- the extract means 1023 extracts the difference of these binary data, and outputs the n-th modification part data 1024. Thereby to the n-th modification part data 1024, the information on which data were deleted in which location between the n-1st modification electronic filing document 1020 and the n-th modification electronic filing document 1022, which data were inserted in which location, or which data were replaced in which location is saved.
[0428] Next, modification person authentication data 1026A of a n-th modification electronic filing document and modification person authentication data 1026B of a n-th modification part are generated, respectively from the authentication line crack, the n-th modification electronic filing document 1022, and the n-th modification part 1024 after the completion of document modification by modification person #n (SS5, drawing 40).
[0429] That is, the n-th modification electronic filing document 1022 is given to modification person authentication means 1025A, and n-th modification person authentication data 1026A is generated. For this reason, description data 1025A-2 of the n-th modification modification electronic filing document 1022 are first extracted by feature-extraction means 1025A-1 (drawing 41). These description data 1025A-2 are data in which the description of the electronic filing document itself it is featureless to the value from which that value differed is shown, even if 1 bit of n-th modification modification electronic-filing-document 1022 throat changes. On the other hand, header 1026 A-H is data added in order to make it it turn out that it is data with which description data 1025A-2 belong to the n-th modification modification electronic filing document 1022.
[0430] Next, it is enciphered by encryption means 1025A-4 using private key 1025A-3 of modification person #n, and description data 1025A-2 are outputted as code data 1026 A-D. Literally, private key 1025A-3 of modification person #n are the key it was made not to tell other than modification person #n, and they accomplish the public key of modification person #n, and a pair. Header 1026 A-H and code data 1026 A-D correspond, and are collectively outputted as modification person authentication data 1026A.
[0431] similarly, the description is extracted from the n-th modification part data 1024 by modification person authentication means 1025B -- a n-th modification person -- difference -- authentication data 1026B is generated.
[0432] Next, a twist is combined with the n-1st modification electronic-filing-document authentication data 1027 taken out from the n-1st modification electronic filing documents 1004 with authentication, modification person authentication data 1026A of the n-th modification electronic filing document, and a coupling means 28, and the joint authentication data 1029 which are the n-th time are generated (SS6, drawing 40 R> 0).
[0433] Next, the n-th joint authentication data 1029 and modification person authentication data 1026B of a n-th modification part are transmitted to the external authentication system 1102 through a network 1100 through the communication device 1129 of the document modification authentication system 1103 (SS7).
[0434] Processing from the following step SS 8 to SS10 is performed in the external authentication system 1102.
[0435] first, the modification person joint authentication data 1029 of a n-th modification document and those [n-th modification] to whom the external authentication system 1102 was sent from the document modification authentication system 1103 -- difference -- authentication data 1026B is

received (SS8).
[0436] Next, in the external authentication system 1102, the n-th sent joint authentication data 1029 and modification person authentication data 1026B of a n-th modification part are attested by the external authentication means 1030A and 1030B, respectively, and the authentication data 1031A and 1031B are generated, respectively (SS9, drawing 40). This processing is explained below.
[0437] For this reason, header 1031 A-H is first taken out from the modification person joint authentication data 1029 of a n-th modification document by external authentication means 1030A. Then, the code data / authentication data 1026 A-D/1027 remaining are given to coupling means 1030A-1 (drawing 42 R> 2).
[0438] External authentication data 1030 A-A (authentication activation ID) of an external certificate authority is combined with these code data / authentication data 1026 A-D/1027 by coupling means 1030A-1. in addition, the thing from which the authentication activation ID as this authentication activation identification information differs for every authentication in principle -- it is -- which authentication -- receiving -- ** -- it is saved in the external certificate authority 1099 whether the authentication activation ID was given.
[0439] Next, this joint data is enciphered by encryption means 1030A-3 using private key 1030A-2 of an external certificate authority, and code data 1031 A-D is generated.
[0440] Here, external authentication data 1030 A-A is information which shows what the external certificate authority which is a third person to the data with which the document modification authentication system 1103 has required authentication attested, and the attested date data are contained. Header 1031 A-H and code data 1031 A-D are outputted as a relating injury line crack of data and n-th modification electronic-filing-document authentication data 1031A.
[0441] the same -- a modification person -- difference -- external authentication also gives authentication data 1026B by external authentication means 1030B -- having -- the n-th time -- difference -- it is outputted as authentication data 1031B. Processing of external authentication means 1030B in this case is explained by reading A of drawing 42 as B.
[0442] namely, instead of receiving the modification person joint authentication data 1029 of a n-th modification document in external authentication means 1030B -- a n-th modification person -- difference -- if data are received from authentication data 1026B, header 1031 B-H will be taken out and remaining code data 1026 B-D will be given to coupling means 1030B-1. External authentication data 1030 B-A of an external certificate authority is combined with said code data 1026 B-D by coupling means 1030B-1, it is enciphered by encryption means 1030B-3 using private key 1030B-2 of an external certificate authority, and code data 1031 B-D is generated. Here, external authentication data 1030 B-A is information which shows what the external certificate authority which is a third person to the data with which the document modification authentication system 1103 has required authentication attested, and the attested date data are contained. header 1031 B-H and code data 1031 B-D -- the n-th time -- difference -- relating of data is performed as authentication data 1031B.
[0443] in this way, generated n-th modification electronic-filing-document authentication data 1031A and the n-th time -- difference -- authentication data 1031B -- the communication device 1129 of the external authentication system 1102 -- minding -- a network 1100 -- a passage -- the document modification authentication system 1103 -- transmitting -- having (SS10) .
[0444] In the document modification authentication system 1103, the data sent from the external authentication system 1102 are received as authentication data 1032A and 1032B, and these received data are given to modification and the authentication means 1006 (SS11).
[0445] Next, in modification and the authentication means 1006, the relating injury line crack by the n-th modification electronic filing document 1022 and the modification electronic filing document 1008 with authentication which is the n-th time are generated, and n-th modification electronic-filing-document authentication data 1031A is outputted. the same -- the n-th time -- difference -- with [whose authentication data 1031B is the relating injury line crack by the n-th modification part data 1024, and

the n-th time] authentication -- difference -- the authentication data 1007 are generated and outputted (SS12, drawing 40).

[0446] Next, it is combined with the modification part data 1003 with authentication from the 1st modification to the n-1st modification by the coupling means 1009, and the modification part data 1007 turn into the modification part data 1010 with authentication from the 1st time to the n-th time with which relating was made respectively by it. Furthermore, the electronic filing document 1011 with n-th modification hysteresis with which the modification part data 1010 with authentication from the 1002 or 1st original electronic filing document with authentication to the n-th time and the modification electronic filing document 1008 with the n-th authentication were connected is generated by the coupling means 1009 (SS13, drawing 3939).

[0447] In addition, if the electronic filing document 1001 with modification hysteresis is made into the n-th electronic filing document with modification hysteresis when changing n+1, the n+1st electronic filing documents with modification hysteresis will be obtained as an electronic filing document 1011 with modification hysteresis.

[0448] As mentioned above, since the alteration prevention system and approach of a modification electronic filing document concerning the gestalt of operation of this invention complete the procedure in which an external certificate authority attests the modification document in which electronic signature was done by the modification person and it was made to perform additional authentication, it is proved by the authentication date of an external certificate authority that the modification person was creating the modification document surely. moreover -- even if it is the case where there is no electronic signature -- a document modification person -- the description data encryption should do with his private key -- since it will be decrypted with the public key corresponding to this, it is attested that it is the document which becomes modification of a document modification person anyway.

[0449] Moreover, if the body of a modification document is altered, the description data which should be extracted from the document after an alteration will change, and the fact of an alteration of the body of a modification document can be detected by becoming a different thing from description data 1025A-2 previously extracted for authentication. Since description data 1025A-2 previously extracted for authentication on the other hand are enciphered by private key 1030A-2 of a certificate authority with authentication data 1030 A-A of an external certificate authority, the alteration of authentication data 1032A given to the modification electronic filing document 1008 with authentication is impossible. Therefore, even if it is him, after external authentication, a document alteration will become impossible.

[0450] Since the modification electronic filing document with weight of the evidence which can prove the justification of a document by this at the place of a trial is generable, it becomes possible the important document conventionally saved in paper, and to electronize a voucher. Moreover, although the advanced technique was needed for the document of the conventional paper judging the existence of an alteration, since the existence of an alteration can be checked only by completing an electronic procedure in the alteration prevention system of an electronic filing document which becomes this invention, the existence of an alteration can be proved easily.

[0451] While storage areas are furthermore reducible with electronization, document transmission to a remote place can carry out now in an instant, and retrieval by the computer can be performed. In this way, improvement in trust of a commercial transaction and speeding up of dealings can be attained.

[0452] Moreover, since a transmission data encryption is performed in the document modification authentication system 1103 or the external authentication system 1102 in the modification document alteration prevention system of this operation gestalt, it is safe even if it uses a public line as a network 1100.

[0453] Furthermore, in the modification document alteration prevention system of this operation gestalt, since the data exchanged between the document modification authentication system 1103 and the external authentication system 1102 are the descriptions (difference data etc.) of the document data instead of document data, the contents of the document data itself do not have the need of passing to a

network 1100 or the external authentication system 1102, and can maintain the secret of document data.
[0454] Furthermore, since the external authentication data which the external certificate authority attested are combined with an original modification electronic filing document and an original modification part and it was made to manage in the form of the document 1011 with modification hysteresis with authentication, the treatment when saving an electronic filing document becomes easy.
[0455] (Gestalt of the 15th operation) This operation gestalt explains the system which takes out authentication information, such as an authentication date which checked Shinsei [the modification electronic filing document 1011 with authentication attested with the 14th operation gestalt], and the external certificate authority attached.
[0456] The alteration prevention system of this modification electronic filing document is constituted as an authentication-text document check system 1104 shown in drawing 36 .
[0457] Drawing 44 is the block diagram showing the example of a hardware configuration of the authentication-text document check system applied to the alteration prevention system of the modification electronic filing document concerning the gestalt of operation of the 15th of this invention, gives the same sign to the same part as drawing 37, and omits the explanation.
[0458] The authentication-text document check system 1104 consists of a document modification authentication system 1103 and same computing system. The difference with the document modification authentication system 1104 is a program of operation stored in the program storing section 1130 of a hard disk drive unit 1128. This program of operation is called and it is stored as an authentication-text document check program 1135 in RAM1119. CPU1117 controls each part according to this authentication-text document check program 1135, and the authentication-text document check system 1104 is realized. Moreover, the point that a software resource and hardware resources join together and a functional implementation means is constituted is the same as that of the case of the document modification authentication system 1103.
[0459] Next, the functional configuration of the alteration prevention system of an electronic filing document is explained using drawing 45 - drawing 47.
[0460] Drawing 45 is drawing showing the functional configuration of the authentication-text document check system applied to the alteration prevention system of the modification electronic filing document of this operation gestalt, and an example of processing flow, gives the same sign to the same part as drawing 39, and omits explanation.
[0461] In this drawing, modification electronic-filing-document 1011B set as the object of an authentication check consists of original electronic-filing-document 1002B, modification electronic-filing-document 1008B, and modification part 1007B#1 - 1007 B#n -1 from the 1st time to the n-th time and 1007B, and this supports the modification electronic filing document 1011 in the 14th operation gestalt.
[0462] On the other hand, the n-th authentication check means 1040, the n-1st authentication check means 1040#n-1, the date check means 1041, 1041#n-1, and the identity judging means 1042 and 1042#n-1 are prepared in the authentication-text document check system 1104. furthermore, the authentication check means 1040 which serves as a repetition part at the authentication-text document check system 1104, the same authentication check means 1043, and the 1- the 13th the same authentication check means 1044 as the thing in an operation gestalt, date check means 1045, and identity judging means 1046 are established.
[0463] moreover -- the authentication-text document check system 1104 -- electronic-filing-document 1011with modification hysteresis B to original electronic-filing-document with authentication 1002B, and with [from the 1st modification to the n-th modification] authentication -- modification part data 1007B#1, 1007B#2, and -- 1007 B#n -1, 1007B, and modification electronic-filing-document 1008with the n-th authentication B are taken out, and a means (not shown) to decompose into authentication data, document data, and modification part data is established.
[0464] Next, each functional configuration of an authentication check means to constitute the

authentication-text document check system 1104 using drawing 46 and drawing 47 is explained.
[0465] Drawing 46 is drawing showing the detail configuration of the authentication check means 1040, and drawing 47 is drawing showing the detail configuration of the authentication check means 1040#n-1.
[0466] The authentication check means 1040 consists of authentication check means 1040A which checks the n-th authentication of modification electronic-filing-document 1008with authentication B, and authentication check means 1040B which checks the n-th authentication of modification part 1007with authentication B.
[0467] In authentication check means 1040A, authentication data 1401A, public key 1402A of the external certificate authority 1099, modification person joint authentication data 1404A containing a header, modification person authentication data 1406A, former authentication data 1407A, a modification person's public key 1408A, description data 1410A, and description data 1412A are held. Moreover, decryption means 1403A, separation means 1405A, decryption means 1409A, feature-extraction means 1411A, and collating means 1413A are prepared.
[0468] Here, modification person joint authentication data 1404A containing a header consists of header 1401 A-H and code data 1401 A-D. Moreover, modification person joint authentication data 1404A containing a header consists of header 1404 A-H and modification person joint authentication data 1404 A-D, and modification person joint authentication data 1404 A-D consists of modification person joint authentication data 1404 A-D1 and authentication data 1404 A-D2 of the external certificate authority 1099 further. Former authentication data 1407A consists of a header and a body of authentication data.
[0469] On the other hand, in authentication check means 1040B, authentication data 1401B, public key 1402B of the external certificate authority 1099, modification person authentication data 1404B containing a header, a modification person's public key 1408B, description data 1410B, and description data 1412B are held. Moreover, decryption means 1403B, decryption means 1409B, feature-extraction means 1411B, and collating means 1413B are prepared.
[0470] Here, modification person authentication data 1401B containing a header consists of header 1401 B-H and code data 1401 B-D. Modification person authentication data 1404B containing a header consists of header 1404 B-H and modification person authentication data 1404 B-D, and modification person authentication data 1404 B-D consists of modification person authentication data 1404 B-D1 and authentication data 1404 B-D2 of the external certificate authority 1099 further.
[0471] Next, the authentication check means 1040#n-1 is explained using drawing 47.
[0472] The authentication check means 1040#n-1 consists of authentication check means 1040A which checks n-1 authentication of the authentication data 1027, and authentication check means 1040B which checks authentication of n-1st modification part 1007 B#n -1 with authentication.
[0473] Although the authentication check means 1040A and 1040B in drawing 47 and the authentication check means 1040A and 1040B in drawing 46 use the same means here, the function which is not used by the authentication check of the authentication data 1027 before n-1 time is omitting illustration.
[0474] Next, actuation of the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained using drawing 45 - drawing 50.
[0475] In this authentication-text document check system 1104, it starts from n-th modification electronic-filing-document 1008with authentication B in electronic-filing-document 1011with modification hysteresis B, the check of sequential authentication is repeated toward the direction of a script from the n-th side, and the identity check of a script, the last document, and the electronic filing document of all modification parts is performed. moreover, the fact of authentication by the external certificate authority 1099 from the external authentication data picked out from authentication data and its authentication date 1045, 1041#1, 1041#2, --1041#n- 1 and 1041 are checked.
[0476] Drawing 48 is the flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[0477] In this drawing, electronic-filing-document 1011with modification hysteresis B is first read

through external storage 1114 and a hard disk drive unit 1128 to the network 1100 (TT1). original electronic-filing-document with the authentication from this electronic-filing-document 1011with modification hysteresis B 1002B, and with [from the 1st modification to the n-th modification] authentication -- modification part data 1007B#1, 1007B#2, and -- 1007 B#n -1, 1007B, and modification electronic-filing-document 1008with the n-th authentication B are taken out, and it is further decomposed into authentication data, document data, and modification part data (TT2).

[0478] Next, the count N of document modification is set as the n last counts of modification, and an authentication check first time flag is set up (TT3).

[0479] Here, it is judged whether it is a first-time authentication check (TT5). In the case of the first time, the authentication data of N time modification document data 1008B, the document data of N time modification document 1008B, the modification authentication data of N time modification part 1007B, and the modification part data of N time modification part 1007B are read into the authentication check means 1040 (TT6).

[0480] Then, an authentication check is performed by the authentication check means 1040, the authentication data 1027 are outputted, and the date authentication data 1041 which included the date of an external certificate authority and the authentication activation ID at least are generated (TT8).

[0481] On the other hand, when it is not the first time at a step TT 5, according to the number of N, either to 1 time modification part 1007B#1 is read into the authentication check means 1040 from n-1st modification part 1007 B#N -1 (TT7).

[0482] Then, an authentication check is performed by the authentication check means 1040#n-1 and 1040#n-2 --, the authentication data 1027 are outputted, and the date authentication data 1041#n-1 and 1041#n-2 -- are generated (TT8). As for the authentication check means 1041#n-1 and 1041#n-2 --, call appearance of the same authentication check means is carried out here repeatedly.

[0483] Here, they are the n-th time and the n-1st time. And the contents of qualification of the step TT 8 in the 1st time are briefly explained from the n-2nd time.

[0484] That is, the authentication check of n-th modification electronic-filing-document 1008with authentication B and modification part 1007with the n-th authentication B is first performed by the authentication check means 1040. Thereby, the authentication data 1027 to the n-1st time are outputted, and the authentication date 1041 of an external certificate authority is outputted. Furthermore, the identity judging 1042 with n-th modification electronic-filing-document 1008B and modification part 1007with the n-th authentication B the same as that of the n-th modification electronic filing document 1008 of the electronic filing document 1011 with modification hysteresis and the modification part 1007 with the n-th authentication is performed.

[0485] Moreover, the authentication check of n-1st modification part 1007 B#n -1 with authentication is performed by the authentication check means 1004#n-1. That is, the authentication data 1027#n-1 to the n-2nd time are outputted, and the authentication date 1041#n-1 of an external certificate authority is outputted. Furthermore, the identity judging 1042#n-1 with modification part 1007 B#n -1 with the n-1st authentications the same as that of the modification part 1007#n-1 with the n-1st authentications of the electronic filing document 1011 with modification hysteresis is performed.

[0486] moreover -- the same -- the authentication check means 1043 -- 1st with [the n-2nd time to] authentication -- based on modification part 1007B#1 to 1007 B#n -2, the authentication data of each time and the authentication date of an external certificate authority are outputted. Furthermore, the identity judging with modification part 1007with authentication B#1 --1007 B#n -2 the same as that of the modification part 1007#1--1007#n-2 with authentication of the electronic filing document 1011 with modification hysteresis is performed.

[0487] When the judgment of the inequality of the authentication activation ID or the identity judging means 1042 is no after the above authentication check [which] (TT8) is performed (TT9), the inequality of N time document is displayed on a display 1111, and is completed. In addition, it may output to external storage 1114, may output to a hard disk drive unit 1128, or it outputs to a network 1100, and

you may end (TT10).
[0488] On the other hand, by the authentication activation ID being in agreement, when the judgment of the identity judging means 1042 is truth (TT9), an authentication check first time flag is cleared and the count N of modification is reduced one (TT11).
[0489] Next, it is judged for the count N of modification whether it is 1 (TT12), when N is larger than 1, it is judged by the step TT 4 whether it is the authentication check of return and the first time (TT5), and a step TT 5 - a step TT 12 are repeated.
[0490] On the other hand, when the count N of modification is 1, the authentication data and document data of original electronic-filing-document with (TT12) authentication 1002B are read into the authentication check means 1044 (TT13). In addition, the authentication data given here are outputted from the authentication check means 1043, and document data remove an authentication part from original electronic-filing-document with authentication 1002B.
[0491] Then, an authentication check is performed by the authentication check means 1044, the date authentication data 1045 of the external certificate authority of a script are outputted, and the identity judging 1046 with original electronic-filing-document 1002B and the the same original electronic filing document 1002 is performed (TT14). In addition, with the authentication check means 1044, since authentication check processing is the same as that of the thing in a previous operation gestalt, explanation is omitted.
[0492] When the judgment of the identity judging means 1046 is no here (TT15), an inharmonious purport is displayed on a display 1111 and original electronic-filing-document 1002B is completed. In addition, it may output to external storage 1114, may output to a hard disk drive unit 1128, or it outputs to a network 1100, and you may end (TT16).
[0493] On the other hand, when the judgment of the identity judging means 1046 is truth (TT15), the purport which is document coincidence, and the modification date from the creation data of a original electronic filing document to a n-th modification document are displayed on a display 1111, and are completed. Moreover, it may output to external storage 1114, may output to a hard disk drive unit 1128, or it outputs to a network 1100, and you may end (TT17). In addition, an authentication date may display both who were obtained by authentication check means 1040A and B, and may display one of the two. Moreover, you may make it judge that both date is in agreement.
[0494] Moreover, you may make it output the identifier of the implementer of a script, and the modification person of each time etc. at a step TT 17.
[0495] The above is the overall processing flow of the authentication-text document check system 1104 in this operation gestalt. Here explains below more concretely about the processing 1040 of the step TT 8 in drawing 48, i.e., an authentication check means, and processing of 1040#n-1.
[0496] Drawing 49 is the flow chart showing processing of authentication check means 1040A in the authentication check system of this operation gestalt.
[0497] Although this drawing shows the authentication check means 1040 and the both sides of processing of 1040#n-1, here explains it taking the case of the case of processing of the authentication check means 1040.
[0498] First, the part of authentication data is inputted into authentication check means 1040A from n-th modification electronic-filing-document 1008with authentication B. This authentication data 1401A is divided into header 1401 A-H understood that n-th it is modification electronic-filing-document 1008with authentication B, and code data 1401 A-D (T801, drawing 46). In addition, n-1 -- If it is in the 1st modification, authentication data and a header before outputting at steps T811 and T812 mentioned later are used as each above-mentioned data.
[0499] Among these, code data 1401 A-D is decoded by decryption means 1403A which used public key 1402A of the external certificate authority 1099, and modification person joint authentication data 1404 A-D is outputted (T802, drawing 46). At this time, modification person joint authentication data 1404 A-D and header 1401 A-H are set to relating eclipse and authentication data 1404A (T803, drawing 46).

[0500] Next, the date data and the authentication activation ID are taken out from external authentication data 1404 A-D2 in modification person joint authentication data 1404 A-D at least, and it is given to the date authentication means 1041 (T804, drawing 46).
[0501] On the other hand, modification person authentication data 1404 A-D1 in modification person joint authentication data 1404 A-D is given to separation means 1405A, and modification person authentication data 1406A and before are separated authentication data 1407A (T805, drawing 46). Here, former authentication data 1407A is data including authentication of the modification document from authentication of a script to n-1 time. Former authentication data 1407A is outputted as authentication data 1027 given to the authentication check means 1040#n-1.
[0502] Next, an authentication check first time flag is checked, when it is the first time, step T807 is performed, and in not being the first time, it moves to step T810 (T806).
[0503] When step T807 is performed, it is decrypted by decryption means 1409A by public key 1408A whose modification person authentication data 1406A is the n-th time of a modification person, and n-th description data 1410A is generated (T807, drawing 46).
[0504] On the other hand, if it is in last round (the n-th time) modification, the part of document data is extracted from the description of reception and document data by feature-extraction means 1411A from modification electronic-filing-document data 1008B, and description data 1412A is outputted (T808, drawing 46). In addition, n-1 -- If it is in the 1st modification, it is the authentication data 1027 and 1027#n-1 -- The description data are extracted from 1027#2.
[0505] Next, description data 1412A by which the feature extraction was carried out to decrypted description data 1410A for the authentication check is collated by collating means 1413A, and the result is outputted to the identity judging means 1042 (T809). When a collating result is judged with the identity judging means 1042 to be coincidence, it is proved that the modification electronic filing document 1008 and modification electronic-filing-document 1008B are in agreement.
[0506] Furthermore, from authentication check means 1040A, former authentication data 1407A is outputted as authentication data 1027 (T811), and header 1404 A-H about this modification is outputted (T812). These are n-1. -- It will be used for authentication of the 1st modification.
[0507] Next, processing of an authentication check means 1040B part is explained among the authentication check means 1040.
[0508] Drawing 50 is the flow chart showing processing of authentication check means 1040B in the authentication check system of this operation gestalt.
[0509] Although this drawing shows the authentication check means 1040 and the both sides of processing of 1040#n-1, here explains it taking the case of the case of processing of the authentication check means 1040.
[0510] First, the part of authentication data is inputted into authentication check means 1040B from n-th modification part 1007with authentication B. This inputted authentication data 1401B is divided into header 1401 B-H and code data 1401 B-D which were understood that n-th it is modification part 1007with authentication B (T821, drawing 46).
[0511] Next, code data 1401 B-D is given to decryption means 1403B, public key 1402B of the external certificate authority 1099 is used and decoded, and modification person authentication data 1404 B-D is generated (T822, drawing 46). Public key 1402B is the thing of the same contents as public key 1402A here.
[0512] Moreover, modification person authentication data 1404 B-D and header 1404 B-H are set to relating eclipse and authentication data 1404B (T823, drawing 46).
[0513] The date data of the external certificate authority 1099 and the authentication activation ID are taken out from external authentication data 1404 B-D2 in modification person authentication data 1404 B-D at least, and it is given to the date authentication means 1041 (T824, drawing 46).
[0514] On the other hand, modification person authentication data 1404 B-D1 in modification person authentication data 1404 B-D is given to decryption means 1409B. In decryption means 1409B, the n-th

modification person's public key 1408B is used, modification person authentication data 1404 B-D1 is decrypted, and description data 1401B of the n-th modification part is taken out (T827, drawing 46). Public key 1408B is the thing of the same contents as public key 1408A here.

[0515] On the other hand, if it is in last round (the n-th time) modification, the part of modification part data is extracted from the description of reception and modification part data by feature-extraction means 1411B from modification part data 1007B, and description data 1412B is outputted (T828, drawing 46). In addition, n-1 -- If it is in the 1st modification, it is the modification part data 1007 and 1007#n-1 -- The description data are extracted from 1007#2.

[0516] Next, description data 1412B by which the feature extraction was carried out to decrypted description data 1410B for the authentication check is collated by collating means 1413B, and the result is outputted to the identity judging means 1042 (T829). When a collating result is judged with the identity judging means 1042 to be coincidence, it is proved that the modification part 1007 and modification part 1007B are in agreement. In addition, when it is the judgment with the result of the collating means of both in authentication check means 1040A and B same [both], more specifically, it is proved that there is no document alteration by the n-1st time to the n-th document modification.

[0517] Furthermore, from authentication check means 1040B, header 1404 B-H about this modification is outputted (T832).

[0518] The above mainly explained the authentication check processing (drawing 48: step T8) by the authentication check means 1040. However, since there is a part which reaches authentication check means 1040#n-1 and is somewhat different from this in the authentication check processing by 1043, the part is explained using drawing 47, drawing 48, and drawing 49.

[0519] First of all, processing by the authentication check means 1040#n-1 is explained.

[0520] n-1 time of the authentication data 1027 outputted from the authentication check means 1040 is given to authentication check means 1040A of the authentication check means 1040#n-1 as authentication data 1401A in drawing 47. If even free comes out and the comparison collating result given to the identity judging means 1042#n-1 removes a certain point, the following processings are the same as that of the case of the authentication check means 1040. In addition, authentication data 1407A in drawing 47 is given to the following authentication check means 1043 as authentication data 1027.

[0521] Moreover, with the authentication check means 1043, the same processing as the authentication check means 1040#n-1 is repeated, and the authentication check from the n-2nd time to the 1st time is performed.

[0522] As mentioned above, the alteration prevention system and approach of a modification electronic filing document concerning the gestalt of operation of this invention addition of the text and the encryption description data from modification #1 to modification #n, and a text implementer and him from modification person #1 to #n -- from the modification electronic filing document by which authentication and authentication of an external certificate authority were made The authentication data of an external certificate authority are taken out from n one by one toward 1. Moreover, since the description data of the document data added and the description data of a modification part, the description data from the electronic-filing-document body for a check, and the description data of a modification part were collated using the public key from document modification person #n to #1 On the authentication date of the external certificate authority for every modification, it can prove that modification person #1 to #n was making a document change surely.

[0523] in addition, the thing which description data 1410A has an alteration prevented by the external certificate authority 1099 on the other hand when description data 1411A extracted from electronic-filing-document 1008B will change, if an electronic-filing-document body is altered -- a modification person -- even if it is him, after external authentication, a document alteration becomes impossible.

[0524] Moreover, modification person #n's substitution of electronic-filing-document 1008B discovers that the authentication activation ID data which the external certificate authority 1099 added by

external authentication means 1030A and external authentication means 1030B have changed or disappeared by the date authentication 1041. Therefore, the substitution concerned is impossible. Moreover, since authentication of text 1002B uses the authentication data 1027#1, the alteration of the text 1002B itself and substitution are also impossible.

[0525] thus, electronic-filing-document 1011with modification hysteresis B -- not only the modification person itself but an external certificate authority, and what other -- it cannot alter a person pair-of-shoes person.

[0526] In the phase of all modification hysteresis, the justification of a document can be proved at the place of a trial from the text of a modification document by this, and the electronization of a voucher is attained also to two or more persons' modification record with the same interests, such as a manufacturer's data report and inspection records.

[0527] Moreover, since authentication of an external certificate authority is performed to the description data, it is safe even if holding a secret to the exterior uses a public line as a network 1100 also to a required document.

[0528] Furthermore, the treatment when saving a document becomes easy by combining the script which the external certificate authority attested, a modification part, and the last document.

[0529] Moreover, since there is no need that the authentication check of modification of each time of a modification document reverts by going back one by one from the last document, the check of authentication can carry out at high speed.

[0530] (Gestalt of the 16th operation) This operation gestalt explains the authentication system of the modification document which is the modification of the 14th operation gestalt. It is a modification about modification and the authentication means 1006 of modification person #n in drawing 39 more correctly.

[0531] Drawing 51 is drawing showing modification in the alteration prevention system of an electronic filing document including document modification of the 16th operation gestalt of this invention, the functional configuration of an authentication means, and processing flow, gives the same sign to the same part as drawing 40, and omits explanation.

[0532] In modification and the authentication means 1006 of modification person #n, replace with modification person authentication means 1025A of drawing 40, and the feature-extraction means 1033 and the modification person authentication means 1034 are established, and also the alteration prevention system of an electronic filing document including document modification shown in drawing 51 is constituted like the 14th operation gestalt.

[0533] Here, the feature-extraction means 1033 is a means to extract the description of the modification document 1022. Moreover, the modification person authentication means 1034 is a means to encipher and attest the joint data outputted from a coupling means 1028 by a modification person's cryptographic key, and to output the authentication data 1029. In addition, the modification person authentication means 1034 is similar with modification person authentication means 1025A of drawing 40, and it is enciphered, without carrying out the feature extraction of the joint data outputted by the coupling means 1028 instead of description data 1025A-2.

[0534] Next, actuation of the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained.

[0535] First, it is the same as that of the 14th operation gestalt till the place where the n-th modification modification electronic filing document 1022 and the authentication data 1027 are obtained from the n-1st modification electronic filing documents 1004 with authentication given to modification and the authentication means 1006.

[0536] Next, the n-th modification electronic filing document 1022 is inputted into the feature-extraction means 1033. The description data generated by this feature-extraction means 1033 are combined with the authentication data 1027 by the coupling means 1028. The data combined by this coupling means 1028 are given to the modification person authentication means 1034, are enciphered, and the modification person joint authentication data 1029 of a n-th modification document are created.

[0537] Hereafter, the same processing as the 14th operation gestalt is performed.
[0538] As mentioned above, the alteration prevention system and approach of a modification electronic filing document concerning the gestalt of operation of this invention Since it had the same configuration as the 14th operation gestalt and also the feature-extraction means 1033 and the modification person authentication means 1034 were established The same effectiveness as the 14th operation gestalt is acquired, and also if the body of a modification document is altered, the description data which should be extracted from the document after an alteration can change, and the fact of an alteration of the body of a modification document can be detected by becoming a different thing from the description data 1033 previously extracted for authentication.
[0539] Moreover, since the description data 1033 previously extracted for authentication on the other hand are enciphered by private key 1030A-2 of a certificate authority with authentication data 1030 A-A of an external certificate authority, the alteration of authentication data 1032A given to the modification electronic filing document 1008 with authentication is impossible. Therefore, even if it is him, after external authentication, a document alteration will become impossible.
[0540] (Gestalt of the 17th operation) This operation gestalt explains the authentication check system of the modification document which is the modification of the 15th operation gestalt. They are the authentication check means 1040 of drawing 45, and a modification about 1040#n-1 more correctly.
[0541] Drawing 52 is drawing showing the functional configuration and processing flow of an authentication check means in the alteration prevention system of an electronic filing document including document modification of the 17th operation gestalt of this invention, gives the same sign to the same part as drawing 45, and omits explanation.
[0542] the alteration prevention system of an electronic filing document including document modification shown in drawing 52 -- the authentication check means 1040 and 1040#n- in 1 and 1043, replace with separation means 1405A, and separation means 1414A is prepared, and also it is constituted like the 15th operation gestalt.
[0543] Next, actuation of the alteration prevention system of the electronic filing document concerning the gestalt of operation of this invention constituted as mentioned above is explained.
[0544] First, in authentication check means 1040A, it is the same as that of the 15th operation gestalt till the place where modification joint authentication data 1404A is obtained.
[0545] Here, modification person joint authentication data 1404 A-D is given to decryption means 1409A, and modification person joint authentication data decode is carried out by the n-th modification person's public key 1408A. Separation means 1414A dissociates further and decode data are set to description data 1410A and authentication data 1407A.
[0546] Hereafter, the same processing as the 15th is performed.
[0547] In addition, it reaches authentication check means 1040#n-1, and same processing is performed also in 1043.
[0548] As mentioned above, since the alteration prevention system and approach of a modification electronic filing document concerning the gestalt of operation of this invention had the same configuration as the 15th operation gestalt, and also were replaced with separation means 1405A and prepared separation means 1414A, they can acquire the same effectiveness as the 15th operation gestalt.
[0549] in addition, in the range which is not limited to the gestalt of each above-mentioned implementation, and does not deviate from the summary, many things are boiled and this invention can be deformed
[0550] For example, although it is expressed only as an electronic filing document 1 with each operation gestalt, if this so-called electronic filing document is electronic intelligence, it not only a document but is good anything. For example, binary data, such as image data, voice data, a program source file, and a program execution file, are also included.
[0551] Furthermore, although the operation gestalt mainly explains the case of a public key

cryptosystem, this invention is not restricted to this and may use a private key cryptosystem.
[0552] Moreover, as a program (software means) which a computer (computer) can be made to execute, the technique indicated in the operation gestalt is stored in storages, such as magnetic disks (a floppy disk, hard disk, etc.), optical disks (CD-ROM, DVD, etc.), and semiconductor memory, and can be transmitted by communication media and can also be distributed. In addition, the setting program which makes the count inside of a plane constitute the software means (for not only an executive program but a table and DS to be included) which a calculating machine is made to perform is also included in the program stored in a medium side. The computer which realizes this equipment reads the program recorded on the storage, and by the case, builds a software means by the setting program, and performs processing mentioned above by controlling actuation by this software means.
[0553]
[Effect of the Invention] according to [as a full account was given above] this invention -- an implementer -- since the electronic filing document which also prevented the alteration by him itself can be offered, the alteration prevention system and approach of an electronic filing document which made it possible to attain employment by the electronic filing document also to what was not able to be employed when it was not paper, and to realize electronization in true semantics conventionally [, such as an important document and an official document,] can be offered.
[0554] Thus, by electronic-filing-document-ization which prevented the alteration, an important document can be sent now within an instant even in a remote place. Moreover, signs can be exchanged within the instant in the location left by implementation of an electronic contract even when a contract was signed. The storage area of a document will not be taken by electronic-filing-document-ization. The effectiveness -- retrieval of a document is attained by electronic-filing-document-ization -- is size very much.
[0555] Moreover, according to this invention, since can observe the contents of the electronic filing document and they cannot be known from the description data of an electronic filing document, an external certificate authority can be attested about the confidential document of a company, and the alteration prevention system and approach of an electronic filing document which can escape the risk of leakage of secrets can be offered.
[0556] Furthermore, according to this invention, the alteration prevention system and approach of an electronic filing document which can create the description data of an electronic filing document at high speed, and can perform compaction of the description data extraction time amount and the transmission time of data since compressibility is also high can be offered.
[0557] enciphering a cryptographic key and a private key further again using fingerprint data according to this invention -- him -- since the data cannot be used for others even if authentication data are sometimes stolen -- him -- the alteration prevention system and approach of an electronic filing document which can make dependability of authentication data very high can be offered.
[0558] Moreover, according to this invention, even when two or more persons draw up one electronic filing document over a term at two or more:00, the need of re-recognizing a modification document by all persons concerned can be abolished, and a document alteration can be prevented, and the alteration prevention system and approach of an electronic filing document whose creation of the electronic filing document which has the weight of the evidence more than the weight of the evidence of a paper document was enabled can be offered.
[0559] Thus, since the modification electronic filing document which also prevented the alteration by the production person itself can be offered, employment of partial modification on an electronic filing document is attained also to what was not able to be employed when it was not paper conventionally [, such as an important document and an official document,]. Moreover, since the contents, a manufacture stage and the contents of modification, and the modification stage of those documents are proved about the data which do not want to indicate to external by the document used in a company, various design data, a design drawing and manufacture data, a working drawing and trial data, a test data,

a test result, inspection data, an inspection result, etc. can be used as very leading trial data when product accident etc. occurs. The check sheet with which the contents are especially added to one sheet of paper over two or more stages by the middle class of a design process, a production process, and an inspection process realizes electronization as data which can prove justification at the place of a trial.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] Drawing showing the overall configuration of the creation system of the electronic filing document in each operation gestalt of this invention, and an approach.
[Drawing 2] The block diagram showing the example of a hardware configuration of the document authentication system applied to the alteration prevention system of the electronic filing document concerning the gestalt of operation of the 1st of this invention.
[Drawing 3] The block diagram showing the example of a hardware configuration of the external authentication system applied to the alteration prevention system of the electronic filing document of this operation gestalt.
[Drawing 4] Drawing showing the functional configuration of the alteration prevention system of the electronic filing document of this operation gestalt, and an example of processing flow.
[Drawing 5] The flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[Drawing 6] The block diagram showing the example of a hardware configuration of the authentication-text document check system applied to the alteration prevention system of the electronic filing document concerning the gestalt of operation of the 2nd of this invention.
[Drawing 7] Drawing showing the functional configuration of the authentication-text document check system applied to the alteration prevention system of the electronic filing document of this operation gestalt, and an example of processing flow.
[Drawing 8] The flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[Drawing 9] Drawing showing the functional configuration of the 3rd of the alteration prevention system of the electronic filing document of the gestalt of operation of this invention, and an example of processing flow.
[Drawing 10] The flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[Drawing 11] Drawing showing the functional configuration of the 4th of the alteration prevention system of the electronic filing document of the gestalt of operation of this invention, and an example of

processing flow.
[Drawing 12] The flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[Drawing 13] Drawing showing the functional configuration of the 5th of the alteration prevention system of the electronic filing document of the gestalt of operation of this invention, and an example of processing flow.
[Drawing 14] The flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[Drawing 15] Drawing showing the functional configuration of the 6th of the alteration prevention system of the electronic filing document of the gestalt of operation of this invention, and an example of processing flow.
[Drawing 16] Drawing showing the functional configuration of the alteration prevention system of the electronic filing document of the 7th operation gestalt of this invention, and an example of processing flow.
[Drawing 17] The flow chart showing electronic seal generation processing of the alteration prevention system of the electronic filing document of this operation gestalt.
[Drawing 18] The flow chart showing electronic verification-of-a-seal-impression processing of the alteration prevention system of the electronic filing document of this operation gestalt.
[Drawing 19] The flow chart showing document header edit processing of the alteration prevention system of the electronic filing document of this operation gestalt.
[Drawing 20] Drawing for explaining the feature-extraction approach in the alteration prevention system of the electronic filing document of the gestalt of operation of the 8th of this invention.
[Drawing 21] Drawing showing the functional configuration of the alteration prevention system of the electronic filing document of this operation gestalt, and an example of processing flow.
[Drawing 22] The flow chart showing an example of processing of the alteration prevention system feature data extraction of the electronic filing document of this operation gestalt.
[Drawing 23] Drawing for explaining the feature-extraction approach in the alteration prevention system of the electronic filing document of the gestalt of operation of the 9th of this invention.
[Drawing 24] Drawing for explaining the feature-extraction approach in the alteration prevention system of the electronic filing document of the gestalt of operation of the 10th of this invention.
[Drawing 25] Drawing showing the functional configuration of the alteration prevention system of the electronic filing document of this operation gestalt, and an example of processing flow.
[Drawing 26] The flow chart showing an example of processing of the alteration prevention system feature data extraction of the electronic filing document of this operation gestalt.
[Drawing 27] Drawing showing the functional configuration of the 11th of the alteration prevention system of the electronic filing document of the gestalt of operation of this invention, and an example of processing flow.
[Drawing 28] The flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[Drawing 29] Drawing showing the functional configuration of the 12th of the alteration prevention system of the electronic filing document of the gestalt of operation of this invention, and an example of processing flow.
[Drawing 30] The flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[Drawing 31] Drawing showing the functional configuration of the 13th of the alteration prevention system of the electronic filing document of the gestalt of operation of this invention, and an example of processing flow.
[Drawing 32] Drawing showing an example of fingerprint data.
[Drawing 33] Drawing showing an example of the data cut down from fingerprint data to the rectangle

field.
[Drawing 34] Drawing having shown a part of example of the pattern made to match.
[Drawing 35] The flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[Drawing 36] the 14- of this invention -- drawing showing the overall configuration of the alteration prevention system of an electronic filing document including document modification in the 17th operation gestalt, and an approach.
[Drawing 37] The block diagram showing the example of a hardware configuration of the document modification authentication system applied to the alteration prevention system of an electronic filing document including document modification concerning the 14th operation gestalt of this invention.
[Drawing 38] The block diagram showing the example of a hardware configuration of the external authentication system applied to the alteration prevention system of an electronic filing document including document modification of this operation gestalt.
[Drawing 39] Drawing showing the functional configuration of the alteration prevention system of an electronic filing document including document modification of this operation gestalt, and an example of processing flow.
[Drawing 40] Drawing showing the functional configuration of the alteration prevention system of an electronic filing document including document modification of this operation gestalt, and an example of processing flow.
[Drawing 41] Drawing showing modification of modification person #n, and the configuration of the modification person authentication means in an authentication means.
[Drawing 42] Drawing showing the configuration of the external authentication means in an external authentication system.
[Drawing 43] The flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[Drawing 44] The block diagram showing the example of a hardware configuration of the authentication-text document check system applied to the alteration prevention system of the modification electronic filing document concerning the gestalt of operation of the 15th of this invention.
[Drawing 45] Drawing showing the functional configuration of the authentication-text document check system applied to the alteration prevention system of the modification electronic filing document of this operation gestalt, and an example of processing flow.
[Drawing 46] Drawing showing the detail configuration of the authentication check means 1040.
[Drawing 47] Drawing showing the detail configuration of the authentication check means 1040#n-1.
[Drawing 48] The flow chart showing actuation of the alteration prevention system of the electronic filing document of this operation gestalt.
[Drawing 49] The flow chart showing processing of authentication check means 1040A in the authentication check system of this operation gestalt.
[Drawing 50] The flow chart showing processing of authentication check means 1040B in the authentication check system of this operation gestalt.
[Drawing 51] Drawing showing modification in the alteration prevention system of an electronic filing document including document modification of the 16th operation gestalt of this invention, the functional configuration of an authentication means, and processing flow.
[Drawing 52] Drawing showing the functional configuration and processing flow of an authentication check means in the alteration prevention system of an electronic filing document including document modification of the 17th operation gestalt of this invention.
[Drawing 53] Drawing showing the conventional method of signing an electronic filing document and judging the identity.
[Description of Notations]
1 -- Electronic filing document

2 -- Feature-extraction means
2T -- Separator table
2W -- Word array
3 -- The description data with a header
3H -- Header
3D -- The description data
4 -- Private key
5 -- Encryption means
6 -- Code data with a header
6H -- Header
6D -- Code data
7 -- Authentication data with a header
7H -- Header
7D -- Code data
7A -- External authentication data
8 -- Private key
9 -- Encryption means
10 -- Complex data
10H -- Header
10D -- Code data
11 -- Complex data
11H -- Header
11D -- Code data
12 -- Electronic filing document with authentication
13 -- Public key
14 -- Decryption means
15 -- Authentication data with a header
15H -- Header
15D -- Code data
15A -- External authentication data
15 A-D -- The date authentication
16 -- Public key
17 -- Decryption means
18 -- The description data with a header
18H -- Header
18D -- The description data
19 -- Electronic filing document
20 -- Feature-extraction means
21 -- The description data
22 -- Collating means
22-J -- Identity judging
23 -- Authentication data with a header
23H -- Header
23D -- Code data
23A -- External authentication data
24 -- Private key
25 -- Encryption means
26 -- Code data with a header
26H -- Header

26D -- Code data
27 -- Code data with a header
27H -- Header
27D -- Code data
28 -- Electronic filing document with authentication
29 -- Public key
30 -- Decryption means
31 -- Authentication data with a header
31H -- Header
31D -- Code data
31A -- External authentication data
31 A-D -- The date authentication
32 -- Authentication data with a header
32H -- Header
32D -- Code data
32A -- External authentication data
33 -- Private key
34 -- Encryption means
35 -- Code data with a header
35H -- Header
35D -- Code data
36 -- Authentication data with a header
36H -- Header
36D -- Code data
36A -- External authentication data
37 -- Private key
38 -- Encryption means
39 -- Code data with a header
39H -- Header
39D -- Code data
40 -- Code data with a header
40H -- Header
40D -- Code data
41 -- Electronic filing document with authentication
42 -- Public key
43 -- Decryption means
44 -- Authentication data with a header
44H -- Header
44D -- Code data
44A -- External authentication data
44 A-D -- The date authentication
45 -- Public key
46 -- Decryption means
47 -- Authentication data with a header
47H -- Header
47D -- Code data
47A -- External authentication data
47 A-D -- The date authentication
48 -- Public key

49 -- Decryption means
50 -- The description data with a header
50H -- Header
50D -- The description data
51 -- Feature-extraction means
52 -- The description data
53 -- Collating means
53-J -- Identity judging
54 -- Print of a seal
55 -- Feature-extraction means
56 -- The description data
58 -- Encryption means
59 -- Encryption print of a seal
60 -- Electronic seal
61 -- The date signature print-of-a-seal information
62 -- Plastic surgery means
63 -- Document display means
64 -- Fingerprint reader
65 -- Fingerprint
66 -- Feature-extraction means
66S -- Logging means
66SD -- Data
66M -- Matching means
66P -- Pattern
66D -- It is data by the single figure.
67 -- The description data
68 -- Password
69 -- A name and ID
70 -- Cryptographic key generation means
71 -- Cryptographic key
72 -- Random number generator
73 -- Private key public key generation means
74 -- Private key
75 -- Public key
76 -- Encryption means
77 -- Encryption private key
78 -- He authentication data
78F -- Fingerprint
78S -- Encryption private key
78K -- Encryption cryptographic key
78P -- Password
78Ns -- A name and ID
79 -- Display means
80 -- Collating means
81 -- Collating means
82 -- Judgment logic
83 -- Decode means
84 -- Cryptographic key
85 -- Collating means

86 -- Decode means
87 -- Fingerprint data extraction means
87F -- The Hara fingerprint data
87A -- Boundary extract means
87E -- Embossing means
87L -- Profile extract means
87B -- Binary-izing
97 98 -- Record medium
99 -- External certificate authority
100 -- Network
101 -- Document authentication system
102 -- External authentication system
103 -- Authentication-text document check system
110 -- Computer
111 -- Display
112 -- Input unit
113 -- Airline printer
114 -- External storage
115 -- Scanner
116 -- CPU bus
117 -- CPU
118 -- ROM
119 -- RAM
120, 121, 122, 123, 124,125,126,127 -- Interface means
128 -- Hard disk drive unit
129 -- Communication device
130 -- Program storing section
131 -- Data storage section
132 -- Working area
133 -- Document authentication program
134 -- External authentication program
135 -- Authentication-text document check program
1001 -- Electronic filing document with modification hysteresis
1002 -- Hara electronic filing document
1002B -- Original electronic filing document for an authentication check
1003 -- Modification part
1004 -- Modification electronic filing document
1005 -- Separation means
1006 -- Modification and authentication means
1007 -- Modification part
1007 B--n time modification parts
-1--n-1 1007 B#n modification part
1008 -- Modification electronic filing document
1008B -- Modification electronic filing document for an authentication check
1009 -- Coupling means
1010 -- Modification part
1011 -- Electronic filing document with modification hysteresis
1011B -- Electronic filing document with modification hysteresis for an authentication check
1020 -- Modification electronic filing document

1021 -- Modification means
1022 -- Modification electronic filing document
1023 -- difference -- an extract means
1024 -- Modification part
1025A, 1025B -- Modification person authentication means
1025A-1 -- Feature-extraction means
1025A-2 -- The description data
1025A-3 -- Modification person #n private key
1025A-4 -- Encryption means
1026A, 1026B -- Modification person authentication data
1026 A-H -- Header
1026 A-D -- Code data
1027 -- Authentication data
1027#n-1 -- Authentication data
1028 -- Coupling means
1029 -- Joint authentication data
1030A, 1030B -- External authentication means
1030 A-A -- External authentication data
1030A-1 -- Coupling means
1030A-2 -- External private key
1030A-3 -- Encryption means
1031A, 1031B -- Authentication data
1031 A-D -- Code data
1031 A-H -- Header
1032A, 1032B -- Authentication data
1033 -- Feature-extraction means
1034 -- Modification person authentication means
1040 -- Authentication check means
1040A, 1040B -- Authentication check means
1040#n-1 -- Authentication check means
1041 -- The date authentication
1041#n-1 -- The date authentication
1042 -- Identity judging
1042#n-1 -- Identity judging
1043 -- Authentication check (repetition)
1044 -- Authentication check means
1045 -- The date authentication
1046 -- Identity judging
1097 1098 -- Record medium
1099 -- External certificate authority
1100 -- Network
1101 -- Document authentication system
1102 -- External authentication system
1103 -- Document modification authentication system
1104 -- Authentication-text document check system
1110 -- Computer
1111 -- Display
1112 -- Input unit
1113 -- Airline printer

1114 -- External storage
1115 -- Scanner
1116 -- CPU bus
1117 -- CPU
1118 -- ROM
1119 -- RAM
1120-1127 -- Interface means
1128 -- Hard disk drive unit
1129 -- Communication device
1130 -- Program storing section
1131 -- Data storage section
1132 -- Working area
1133 -- Document modification authentication program
1134 -- External authentication program
1135 -- Authentication-text document check program
1401A -- Authentication data
1401 A-D -- Code data
1401 A-H -- Header
1402A -- Public key of an external certificate authority
1403A -- Decryption means
1404A -- Modification person joint authentication data
1404 A-D -- Modification person joint authentication data
1404 A-D1 -- Modification person authentication data
1404 A-D2 -- External authentication data
1404 A-H -- Header
1405A -- Separation means
1406A -- Modification person authentication data
1407A -- Former authentication data
1408A -- A modification person's public key
1410A -- The description data
1411A -- Feature-extraction means
1412A -- The description data
1413A, 1413B -- Collating means
1414A -- Separation means
S -- Electronic-filing-document data list
S1, S2, S3 -- Electronic-filing-document data list part
S_sum -- Total value
S_s_stream -- Sum total data list
IS -- Data list which kept spacing
IS1; IS2, IS3 -- Data list part which kept spacing
IS_sum [0], .., IS_sum [255] -- Array of the total value of the data which kept spacing
IS_s_stream -- Sum total data list which kept spacing
i, j -- Counter

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平11－261550

(43)公開日　平成11年(1999)９月24日

(51)Int.Cl.[6]		識別記号	FI	
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ　9/00	６７５Ｂ
Ｇ０６Ｆ	12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｚ
	17/21		Ｇ０９Ｃ　1/00	６４０Ｂ
Ｇ０９Ｃ	1/00	６４０	Ｇ０６Ｆ　15/20	５７０Ｍ
			Ｈ０４Ｌ　9/00	６７３Ｄ

審査請求　未請求　請求項の数37　ＯＬ　（全 65 頁）　最終頁に続く

(21)出願番号　特願平10－271541

(22)出願日　平成10年(1998)９月25日

(31)優先権主張番号　特願平10－717

(32)優先日　平10(1998)１月６日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　小野　和輝
東京都府中市東芝町１番地　株式会社東芝府中工場内

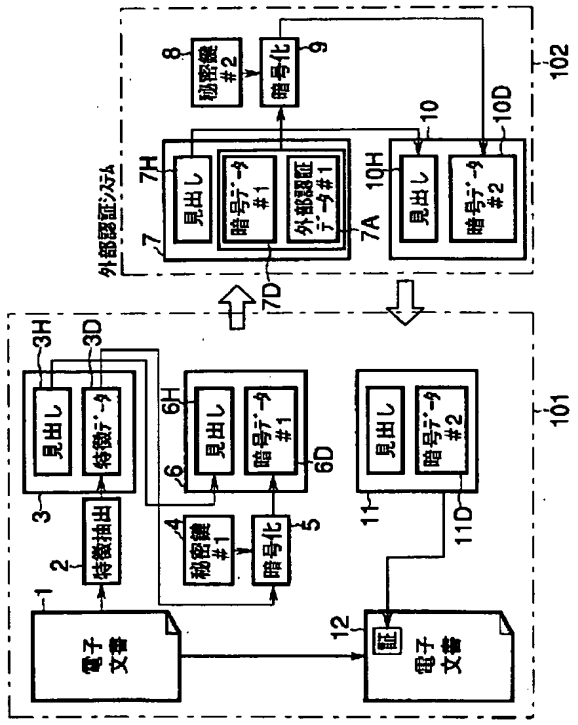
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　電子文書の改竄防止システム及び方法

(57)【要約】

【課題】　本発明は、電子文書に証拠能力を付与するとともに、真の意味での文書の電子化を推進することを可能とする。

【解決手段】　電子文書から特徴を抽出して特徴データを生成する特徴抽出手段１１と、特徴データを第１の当事者の第１の暗号鍵で暗号化し、第１の暗号化データを生成する第１の暗号化手段５と、第１の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを外部認証者の第２の暗号鍵で暗号化して第２の暗号化データを生成する第２の暗号化手段９と、第２の暗号化データを電子文書の認証データとする手段Ｓ１４とを備えた電子文書の改竄防止システム。



1

【特許請求の範囲】

【請求項１】　電子文書から特徴を抽出して特徴データを生成する特徴抽出手段と、

前記特徴データを第１の暗号鍵で暗号化して第１の暗号化データを生成する第１の暗号化手段と、

前記第１の暗号化データに、外部認証データを付加し、これを第２の暗号鍵で暗号化して第２の暗号化データを生成する第２の暗号化手段と、

前記第２の暗号化データを前記電子文書の認証データとする手段とを備える電子文書の改竄防止システム。

【請求項２】　電子文書から特徴を抽出して特徴データを生成する特徴抽出手段、前記特徴データを第１の暗号鍵で暗号化して第１の暗号化データを生成する第１の暗号化手段、前記第１の暗号化データを送信するとともに認証データを受信する第１の通信手段、および前記認証データを前記電子文書に対応させる手段とを備える文書認証システムと、

前記第１の通信手段にて送信される前記第１の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを第２の暗号鍵で暗号化して第２の暗号化データを生成する第２の暗号化手段、および前記第１の暗号化データを受信するとともに前記第２の暗号化データを認証データとして前記文書認証システムに送信する第２の通信手段を備える外部認証システムと、を備えた電子文書の改竄防止システム。

【請求項３】　前記第１の暗号化データを第３の暗号鍵で暗号化して第３の暗号化データを生成する第３の暗号化手段を備え、前記第２の暗号化手段は、前記第１の暗号化データに代えて、前記第３の暗号化データに外部認証データを付加して第２の暗号鍵で暗号化して第２の暗号化データを生成することを特徴とする請求項１又は２記載の電子文書の改竄防止システム。

【請求項４】　前記第２の暗号化データを、前記第２の暗号鍵とは異なる第４の暗号鍵で暗号化して第４の暗号化データを生成し、前記認証データとする第４の暗号化手段をを備えることを特徴とする請求項１，２又は３記載の電子文書の改竄防止システム。

【請求項５】　認証対象の電子文書に対応する認証データから第２の暗号化データを取り出し、これを第２の暗号鍵に対応する第２の公開鍵で復号化する第２の復号化手段と、

前記第２の復号化手段により復号化されたデータから第１の暗号化データを取り出し、これを第１の暗号鍵に対応する第１の公開鍵で復号化する第１の復号化手段と、

前記電子文書から特徴を抽出して照会用特徴データを生成する特徴抽出手段と、

前記第１の復号化手段により復号化されたデータから特徴データを取り出し、前記照会用特徴データと照合する照合手段とを備えたことを特徴とする認証文書確認システム。

2

【請求項６】　請求項５において、前記第２の復号化手段により復号化されたデータから第３の暗号化データを取り出し、これを第３の暗号鍵に対応する第３の公開鍵で復号化する第３の復号化手段を設け、

前記第１の復号化手段は前記第３の復号化手段により復号化されたデータから第１の暗号化データを取り出し、これを第１の暗号鍵に対応する第１の公開鍵で復号化することを特徴とする認証文書確認システム。

【請求項７】　特徴抽出対象データを１単位づつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第１の合計値列とする第１列生成手段と、

この１単位づつ読み出した値に対して前記規定の単位数だけ隔てた関係となる１単位づつ読み出した値を加算し、この加算した値に対して前記関係となる１単位づつ読み出した値を加算し、この加算を繰り返し、合計加算回数として前記規定の単位数回の加算を行って得られる合計値を順次並べて第２の合計値列とする第２列生成手段と、

前記第１の合計値列及び前記第２の合計値列を特徴データとして出力する手段とを備えたことを特徴とする特徴抽出装置。

【請求項８】　前記第１の合計値列を１単位づつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第３の合計値列とする第３列生成手段と、

前記第２の合計値列を１単位づつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第４の合計値列とする第４列生成手段と、

前記第３の合計値列及び前記第４の合計値列を特徴データとして出力する手段とを備えたことを特徴とする請求項７記載の特徴抽出装置。

【請求項９】　指紋読取手段と、

前記指紋読取手段で読み取った指紋データから特徴抽出を行い指紋特徴データを生成する指紋特徴抽出手段と、

前記指紋特徴データ及びパスワードから暗号鍵を生成する暗号鍵生成手段と、

前記指紋特徴データ、パスワード及び乱数値から秘密鍵及び公開鍵を生成する秘密鍵公開鍵生成手段と、

前記暗号鍵で前記暗号鍵自身と前記秘密鍵をそれぞれ暗号化する暗号化手段と、

前記暗号化手段で暗号化したデータ、指紋データ及びパスワードを本人認証データとする手段とを備えたことを特徴とする本人認証データ生成システム。

【請求項１０】　前記請求項９に記載された本人認証データ生成システムで生成した前記本人認証データ中のパスワードと、入力されたパスワードとを照合するパスワード照合手段と、

指紋読取手段と、

両パスワードが一致した場合には、前記指紋読取手段で

指紋読み取りを行い、前記本人認証データ中の指紋データと、前記指紋読取手段にて読み取られた指紋データとを照合する指紋照合手段と、
指紋照合が一致した場合には、前記本人認証データ中の指紋データから特徴抽出を行い指紋特徴データを生成する指紋特徴抽出手段と、
前記指紋特徴抽出手段にて生成された指紋特徴データ及びパスワードから暗号鍵を生成する暗号鍵生成手段と、
この生成された暗号鍵により本人認証データ内の暗号化された暗号鍵を復号して、前記生成された暗号鍵と復号した暗号鍵とを照合する暗号鍵照合手段と、
暗号鍵照合が一致した場合には、この暗号鍵を用いて前記本人認証データ中の暗号化した秘密鍵を復号する秘密鍵復号手段とを備えた秘密鍵復号システム。

【請求項１１】　指紋読取手段と、
前記指紋読取手段から読み取られる指紋データの境界を検出する境界検出手段と、
前記境界検出手段により境界検出された指紋データをエンボス処理するエンボス手段と、
前記エンボス手段によりエンボス処理された指紋データを輪郭トレースする輪郭トレース手段とを備えたことを特徴とする指紋データ抽出装置。

【請求項１２】　前記請求項１１に記載された指紋データ抽出装置から抽出された指紋データから複数の矩形領域を取り出す領域取出手段と、
前記矩形領域のデータと予め登録した複数パターンとを比較し、何れかのパターンとマッチングするか否かを判定するパターンマッチング手段と、
マッチングしたパターンに対応する数値を数列として並べ、当該数列を指紋特徴データとする手段とを備えたことを特徴とする指紋特徴抽出装置。

【請求項１３】　電子文書から特徴を抽出して特徴データを生成する特徴抽出ステップと、
前記特徴データを第１の当事者の第１の暗号鍵で暗号化し、第１の暗号化データを生成する第１の暗号化ステップと、
前記第１の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを外部認証者の第２の暗号鍵で暗号化して第２の暗号化データを生成する第２の暗号化ステップと、
前記第２の暗号化データを前記電子文書の認証データとするステップとを有することを特徴とする電子文書の改竄防止方法。

【請求項１４】　電子文書から抽出したデータを第１の暗号鍵で暗号化して第１の暗号化データを生成する文書認証システムと、受信データを第２の暗号鍵で暗号化して第２の暗号化データを生成する外部認証システムとが通信回線で接続される電子文書の改竄防止システムであって、
文書認証システムにて生成した前記第１の暗号化データを、前記通信回線を介して前記外部認証システムに送信し、
外部認証システムでは、受信した前記第１の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを第２の暗号鍵で暗号化して第２の暗号化データを生成し、この第２の暗号化データを認証データとして前記文書認証システムに送信し、
文書認証システムでは、受信した前記第２の暗号化データを認証データとして前記電子文書に対応させることを特徴とする電子文書の改竄防止方法。

【請求項１５】　第１の文書認証システムにて、電子文書から抽出したデータを第１の暗号鍵で暗号化して第１の暗号化データを生成し、第２の文書認証システムに送信し、
第２の文書認証システムにて、前記第１の文書認証システムより送信された前記第１の暗号化データを第３の暗号鍵で暗号化して第３の暗号化データを生成し、外部認証システムに送信し、
外部認証システムにて、前記第２の文書認証システムより送信された前記第３の暗号化データに外部認証データを付加し、これを第２の暗号鍵で暗号化して第２の暗号化データを生成し、少なくとも前記第１の文書認証システムに送信し、
当該第１の文書認証システムにて、受信した前記第２の暗号化データを認証データとして前記電子文書に対応させることを特徴とする電子文書の改竄防止方法。

【請求項１６】　前記請求項１，２又は３記載の電子文書の改竄防止システムにて生成された前記認証データから前記第２の暗号化データを取出し、これを前記第２の秘密鍵に対応する第２の公開鍵で復号化する第２の復号化ステップと、
前記第２の復号化ステップにより復号化されたデータから前記第１の暗号化データを取出し、これを前記第１の秘密鍵に対応する第１の公開鍵で復号化する第１の復号化ステップと、
前記電子文書から特徴を抽出して照合用特徴データを生成する特徴抽出ステップと、
前記第１の復号化ステップにより復号化されたデータから前記特徴データを取出し、これを前記照合用特徴データと照合する照合ステップと、
前記照合ステップによる照合結果と、前記第２の復号化手段により復号化されたデータから取り出された前記外部認証データによって、外部認証者による認証の事実及び認証の日付を出力するステップとを有することを特徴とする認証文書確認方法。

【請求項１７】　電子文書から特徴を抽出して特徴データを生成する特徴抽出手段と、
前記特徴データを第１の当事者の第１の暗号鍵で暗号化し、第１の暗号化データを生成する第１の暗号化手段と、

前記第１の暗号化データに、少なくとも日付を含む外部認証データが付加され、これが外部認証者の第２の暗号鍵によって暗号化されてなる第２の暗号化データが入力されるとともに、この第２の暗号化データを前記電子文書の認証データとする手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１８】　前記請求項１，２又は３記載の電子文書の改竄防止システムにて生成された前記認証データから前記第２の暗号化データを取出し、これを前記第２の秘密鍵に対応する第２の公開鍵で復号化する第２の復号化手段と、

前記第２の復号化手段により復号化されたデータから前記第１の暗号化データを取出し、これを前記第１の秘密鍵に対応する第１の公開鍵で復号化する第１の復号化手段と、

前記電子文書から特徴を抽出して照合用特徴データを生成する特徴抽出手段と、

前記第１の復号化手段により復号化されたデータから前記特徴データを取出し、これを前記照合用特徴データと照合する照合手段と、

前記照合手段による照合結果と、前記第２の復号化手段により復号化されたデータから取り出された前記外部認証データによって、外部認証者による認証の事実及び認証の日付を出力する手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１９】　電子文書から特徴が抽出されて特徴データが生成され、

次に、前記特徴データが第１の当事者の第１の暗号鍵で暗号化され、第１の暗号化データが生成され、

次に、前記第１の暗号化データに、少なくとも日付を含む外部認証データが付加されて、これが外部認証者の第２の暗号鍵で暗号化して第２の暗号化データが生成され、

最終的に、前記第２の暗号化データからなる構造を有するデータが記録されたコンピュータ読み取り可能な記録媒体。

【請求項２０】　電子文書から特徴が抽出されて特徴データが生成され、

次に、前記特徴データが第１の当事者の第１の暗号鍵で暗号化され、第１の暗号化データが生成され、

次に、前記第１の暗号化データが第２の当事者の第３の暗号鍵で暗号化され、第３の暗号化データが生成され、

次に、前記第３の暗号化データに、少なくとも日付を含む外部認証データが付加されて、これが外部認証者の第２の暗号鍵で暗号化して第２の暗号化データが生成され、

最終的に、前記第２の暗号化データからなる構造を有するデータが記録されたコンピュータ読み取り可能な記録媒体。

【請求項２１】　認証付き電子文書から電子文書を取り出して、これに変更を加えて、新たな電子文書を生成する文書変更手段と、

前記認証付き電子文書から取り出された元の電子文書と前記新たな電子文書との変更点を抽出して変更箇所データを取得する差分抽出手段と、

前記変更箇所データと前記新たな電子文書とをそれぞれ変更者認証する変更者認証手段と、

前記変更者認証手段により認証された各データを外部の認証システムに送出するとともに、それぞれを外部認証された認証データを受け取って、受け取った各認証データ及び前記新たな電子文書に基づいて、認証付き変更箇所データと新たな認証付き電子文書を生成する認証手段とを備えたことを特徴とする電子文書の改竄防止システム。

【請求項２２】　前記変更者認証手段は、

前記変更箇所データ及び又は前記新たな電子文書から特徴抽出して特徴データを出力する特徴抽出手段と、

前記特徴データを、前記新たな電子文書を生成した変更者の暗号化鍵で暗号化して出力する暗号化手段とを備えたことを特徴とする請求項２１記載の電子文書の改竄防止システム。

【請求項２３】　前記変更者認証手段は、

前記暗号化手段から出力されかつ前記新たな電子文書に対応する暗号化特徴データと、元の認証付き電子文書から取り出された以前の認証データとを結合して出力する結合手段を備えたことを特徴とする請求項２２記載の電子文書の改竄防止システム。

【請求項２４】　前記変更者認証手段は、

前記特徴抽出手段により特徴抽出された特徴データと、元の認証付き電子文書から取り出された以前の認証データとを結合して出力する結合手段を備え、

前記暗号化手段の暗号化対象として、前記結合手段からの出力データを前記特徴データに代えて入力することを特徴とする請求項２２記載の電子文書の改竄防止システム。

【請求項２５】　前記請求項２１乃至２４のうち何れか１項に記載された認証手段により生成された認証付き変更箇所データと認証付き電子文書とを含む変更済電子文書から、前記認証付き変更箇所データ及び前記認証付き電子文書を取り出す分離手段と、

前記請求項２１乃至２４のうち何れか１項に記載された文書変更手段、差分抽出手段、変更者認証手段及び認証手段と、

前記認証手段により生成された新たな認証付き変更箇所データ及び新たな認証付き電子文書と、前記分離手段で分離された元の認証付き変更箇所データとに基づき、新たな変更済電子文書を生成する結合手段とを備えたことを特徴とする電子文書の改竄防止システム。

7

【請求項２６】　前記請求項２１乃至２４のうち何れか１項に記載された前記変更者認証手段により認証された各データを受け取る受入手段と、
前記各データそれぞれに、少なくとも日付データ及び認証実行識別情報を結合する結合手段と、
この結合手段により結合された各データを外部認証機関の暗号鍵によって暗号化して、外部認証された認証データを作成する暗号化手段とを備えたことを特徴とする電子文書の外部認証システム。

【請求項２７】　前記請求項２６に記載の外部認証システムにより外部認証された認証データを、外部認証機関の復号鍵で復号する復号化手段と、
前記復号化手段により復号された認証データから、前記日付データ及び前記認証実行識別情報を取り出すデータ取出手段とを備えたことを特徴とする認証文書確認システム。

【請求項２８】　前記請求項２６に記載の外部認証システムにより外部認証された認証データが前記請求項２３に対応しかつ電子文書に対応するものである場合に、
前記復号化手段により復号された認証データから、前記以前の認証データを取り出す認証データ取出手段を備えたことを特徴とする請求項２７記載の認証文書確認システム。

【請求項２９】　前記復号化手段により復号された認証データのうち、前記請求項２２の暗号化手段で暗号化された暗号データが入力されるとともに、当該暗号データを変更者の復号鍵で復号して特徴データを取り出す第２の復号化手段と、
前記請求項２１の文書変更手段で得られた新たな電子文書から特徴抽出して比較用特徴データを出力する特徴抽出手段と、
前記第２の復号化手段で得られた特徴データと、前記特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えたことを特徴とする請求項２８記載の認証文書確認システム。

【請求項３０】　前記請求項２６に記載の外部認証システムにより外部認証された認証データが前記請求項２４に対応しかつ電子文書に対応するものである場合に、
前記復号化手段により復号された認証データを変更者の復号鍵で復号する第２の復号化手段と、
前記第２の復号化手段で復号化された認証データから、前記以前の認証データを取り出す認証データ取出手段とを備えたことを特徴とする請求項２７記載の認証文書確認システム。

【請求項３１】　前記第２の復号化手段で復号化された認証データから、特徴データを取り出す分離手段と、
前記請求項２１の文書変更手段で得られた新たな電子文書から特徴抽出して比較用特徴データを出力する特徴抽出手段と、
前記分離手段で得られた特徴データと、前記特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えたことを特徴とする請求項３０記載の認証文書確認システム。

8

【請求項３２】　前記請求項２６に記載の外部認証システムにより外部認証された認証データが前記請求項２２に対応しかつ前記変更箇所データに対応するものである場合に、
前記復号化された認証データのうち、前記請求項２２の暗号化手段で暗号化された暗号データが入力されるとともに、当該暗号データを変更者の復号鍵で復号して特徴データを取り出す第２の復号化手段と、
前記請求項２１の差分抽出手段で得られた変更箇所データから特徴抽出して比較用特徴データを出力する特徴抽出手段と、
前記第２の復号化手段で得られた特徴データと、前記特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えたことを特徴とする請求項２７記載の認証文書確認システム。

【請求項３３】　前記請求項２５に記載された電子文書の改竄防止システムにより作成された変更済電子文書の変更部分についての認証確認を行うシステムであって、
前記請求項２８又は３０の認証文書確認システムと、前記請求項３２の認証文書確認システムとを備えるとともに、
複数回の変更を受けた最終的な変更済電子文書における認証付き電子文書から、最終変更回に関する認証データを取り出し、まずこれを前記請求項２６に記載の外部認証システムにより外部認証された認証データとして前記請求項２８又は３０の認証文書確認システムに入力し、
最終変更回以外の各回については、前記請求項２８又は３０の認証文書確認システムから出力される前記以前の認証データを、前記請求項２６に記載の外部認証システムにより外部認証された認証データとして、順次、前記請求項２８又は３０の認証文書確認システムに入力し、
また、複数回の変更を受けた最終的な変更済電子文書から、各回の認証付き変更箇所データを取り出し、この認証付き変更箇所データを変更箇所データ及び前記請求項２６に記載の外部認証システムにより外部認証された認証データに分離して、前記請求項３２の認証文書確認システムに入力し、
前記請求項２８又は３０の認証文書確認システムから得られた日付データ及び認証実行識別情報と、前記請求項３２の認証文書確認システムから得られた日付データ及び認証実行識別情報とを各変更回毎に照合することを特徴とする変更済電子文書の認証確認システム。

【請求項３４】　前記請求項２９又は３１の認証文書確認システムを備えるとともに、
最終的な変更済電子文書に包含される認証付き電子文書から取り出された認証データ及び新たな電子文書を、前記請求項２８又は３０の認証文書確認システムに代えて

前記請求項２９又は３１の認証文書確認システムに入力することを特徴とする請求項３３記載の変更済電子文書の認証確認システム。

【請求項３５】　認証付き電子文書から電子文書を取り出して、これに変更を加えて、新たな電子文書を生成する文書変更手段と、

前記認証付き電子文書から取り出された元の電子文書と前記新たな電子文書との変更点を抽出して変更箇所データを取得する差分抽出手段と、

前記変更箇所データと前記新たな電子文書とをそれぞれ変更者認証する変更者認証手段と、

前記変更者認証手段により認証された各データを外部の認証システムに送出するとともに、それぞれを外部認証された認証データを受け取って、受け取った各認証データ及び前記新たな電子文書に基づいて、認証付き変更箇所データと新たな認証付き電子文書を生成する認証手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項３６】　前記変更者認証手段は、

前記変更箇所データ及び又は前記新たな電子文書から特徴抽出して特徴データを出力する特徴抽出手段と、

前記特徴データを、前記新たな電子文書を生成した変更者の暗号化鍵で暗号化して出力する暗号化手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な請求項３５記載の記録媒体。

【請求項３７】　前記請求項２６に記載の外部認証システムにより外部認証された認証データを、外部認証機関の復号鍵で復号する復号化手段と、

前記復号化手段により復号された認証データから、前記日付データ及び前記認証実行識別情報を取り出すデータ取出手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明はデータや文書等の電子文書の改竄を防止し、特に電子文書の証拠能力を確保する部分に特徴のある電子文書の改竄防止システム及び方法に関するものである。

【０００２】

【従来の技術】従来から取引記録、品質記録あるいは契約書等の文書は、文書改竄の疑惑を防止する為に、黒インクやボールペン等を用いて紙上に記入し署名や捺印を行っている。

【０００３】このように紙にインクで記載したものは、後に記載内容や日付を改竄しようとしても容易には改竄できない。紙は古くなると質が変化する為に、新しく偽の文書を作成しても判別が可能である。こうした紙とインクの特徴の為に、従来から重要文書は全て紙で保管されている。

【０００４】最近、電子署名技術が開発され、文書を作成した本人を証明する事ができるようになっている。この電子署名を説明する。

【０００５】図５３は電子文書に署名してその同一性を判定する従来の方法を示す図である。

【０００６】同図に示すように、まず、電子文書２０１ａから特徴抽出手段２０２で特徴データ２０３Ｄを取り出す。次に、この特徴データ２０３Ｄを秘密鍵２０４を用い、暗号化手段２０５により暗号化して暗号データ２０６Ｄを作成する。そして、この暗号データ２０６Ｄを元の電子文書２０１ａと一緒にして署名済み電子文書２０１ｂとして受取人に送信する。

【０００７】受取人は、受け取った電子文書２０１ｂ’から暗号データ２０６Ｄを取り出して送信者の公開鍵２１６を使用し復号化手段２１７により特徴データ２１８Ｄを取り出す。一方、電子文書２０１ｂ’から元の電子文書２０１ａに相当する電子文書２０１ａ’を取り出し、さらに特徴抽出手段２２０により特徴データ２２１を取り出す。特徴データ２２１を先の特徴データ２１８Ｄと照合手段２２により照合し本人の電子文書に相違無い事を確認する。

【０００８】このような電子文書であれば、その文書作成者は間違いなく本人である事を確認できる。しかし、作成者本人であれば、作成済みの文書を自由に改変することが可能である。したがって、作成者本人が、例えばコンピュータの日付を故意にずらせて文書の作成日付を護魔化す等の問題を生じ得る。

【０００９】ここで、特願平5-303773号公報に記載される「電子化文書処理システムおよびディジタル署名の生成方法」では、作成した文書に別の作者が一部変更を加えて、新しい文書にする時の認証方法が開示されている。

【００１０】しかし、作成した電子文書を、作成に関わった作者等以外の利害の対立する者に対して証拠書類として使用することは、作成に関わった作者等が共謀して改竄を行なえば証拠改竄が可能となることから適切とはいえない。すなわち特願平5-303773号公報の方法は、文書を証拠書類として電子化させることには馴染まず、社内文書を社内で使用する場合に限った電子化といえる。

【００１１】例えば製品の製造工程に従って、工程毎の担当者が、自分の担当工程に署名捺印を行なう組み立て記録等には適用できず、紙での運用となっている。また、定期検査の記録で、記録シートに数行の点検結果を追記して署名捺印を行なう場合にも、紙での運用になっていた。この様な物は製品安全の事故に対して、検査記録を証拠とする必要があり、共謀すれば改竄できる電子文書では証拠とはなり得なかった為である。

【００１２】

【発明が解決しようとする課題】このように文書作成者

本人は文書改竄を行う事ができるので、取引記録、品質記録あるいは契約書等の電子文書を本人が改竄していないことが証明できない。このため、現状のシステムでは電子文書に対する信用性は低く、重要書類は相変わらず紙で取り扱われている。

【００１３】しかし、紙の文書は保管に多くの場所を必要とし、必要な文書を取り出すのに時間が掛かる。また、遠方に送る時に本紙と同じ証拠能力を持つ必要が有る場合には、本紙を送る以外に方法が無い問題がある。

【００１４】一方、最近のコンピュータの発達で文書がワープロなどで作成される様になると、紙の形で保管しておくよりも、電子文書として保管する方が便利である。たとえば保管場所を取らない、必要な文書の検索が容易である等の利点を有する為であり、このため文書の電子化が社会一般的に進んで来ている。

【００１５】しかし、上記したように電子文書の証拠能力が不足している事から、重要文書の電子化ができず、たとえ電子化しても、証拠能力を有する紙文書が本紙として別途必要である。このため、重要文書に関しての保管場所が必要である等の問題は依然として解決されない。

【００１６】本発明は、このような実情を考慮してなされたもので、本来紙文書の特徴である証拠能力を電子文書に付与するとともに、真の意味での文書の電子化を推進することを可能とし、ひいては、文書の保管場所の削減、文書の検索の効率化、本紙の文書の遠方への即時配達等を実現できる電子文書の改竄防止システム及び方法を提供することを目的とする。

【００１７】また、本発明の他の目的は、複数人が複数時期に渡って一つの電子文書を作成する場合でも、変更文書を関係者全員で再承認する必要をなくしかつ文書改竄を防止して、紙文書の証拠能力以上の証拠能力を有する電子文書を作成可能とした電子文書の改竄防止システム及び方法を提供することにある。

【００１８】

【課題を解決するための手段】本発明の骨子は、電子文書から抽出された特徴データを第１当事者の暗号鍵で暗号化し、さらにこの暗号化された特徴データを外部認証者の暗号鍵で暗号化してその結果得られた暗号データを電子文書の認証データとして用いるところにある。

【００１９】このようにして得られる認証データは、他人によって改竄することはできないし、暗号化された特徴データを渡された悪意の外部認証者によっても改竄できない。つまり特徴データ自体に第１当事者の暗号がかけれているため、外部認証者がこれを改竄すれば電子文書が正当でないことが検出されるものである。さらに、一度外部認証された認証データは、外部認証者による暗号化のために、第１当事者本人によっても改竄することが不能となる。

【００２０】一方、もとの電子文書を改竄した場合には、改竄電子文書からの特徴データと、認証データに含まれる特徴データとの比較により、その改竄の事実が検出される。

【００２１】このように、本発明では、悪意の他人による場合はもちろんのこと、悪意の第１当事者、さらには悪意の外部認証者のいずれによる場合であっても、もし電子文書又は認証データが何れの段階で改竄されれば、どの段階で改竄が行われた場合であってもその改竄事実が検出される。

【００２２】また、上記課題の解決は、より具体的には、以下のような解決手段により実現される。

【００２３】まず、請求項１に対応する発明は、電子文書から特徴を抽出して特徴データを生成する特徴抽出手段と、特徴データを第１の暗号鍵で暗号化して第１の暗号化データを生成する第１の暗号化手段と、第１の暗号化データに、外部認証データを付加し、これを第２の暗号鍵で暗号化して第２の暗号化データを生成する第２の暗号化手段と、第２の暗号化データを電子文書の認証データとする手段とを備える電子文書の改竄防止システムである。

【００２４】本発明はこのような手段を設けたので、本来紙文書の特徴である証拠能力を電子文書に付与するとともに、真の意味での文書の電子化を推進することを可能とし、ひいては、文書の保管場所の削減、文書の検索の効率化、本紙の文書の遠方への即時配達等を実現することができる。

【００２５】次に、請求項２に対応する発明は、電子文書から特徴を抽出して特徴データを生成する特徴抽出手段、特徴データを第１の暗号鍵で暗号化して第１の暗号化データを生成する第１の暗号化手段、第１の暗号化データを送信するとともに認証データを受信する第１の通信手段、および認証データを電子文書に対応させる手段とを備える文書認証システムと、第１の通信手段にて送信される第１の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを第２の暗号鍵で暗号化して第２の暗号化データを生成する第２の暗号化手段、および第１の暗号化データを受信するとともに第２の暗号化データを認証データとして文書認証システムに送信する第２の通信手段を備える外部認証システムと、を備えた電子文書の改竄防止システムである。

【００２６】本発明はこのような手段を設けたので、請求項１の発明と同様な効果が得られる他、通信回線を用いることで、第１の当事者と外部認証者と間で認証データ作成作業を便利かつ短時間に進めることができる。

【００２７】次に、請求項３に対応する発明は、請求項１又は２に対応する発明において、第１の暗号化データを第３の暗号鍵で暗号化して第３の暗号化データを生成する第３の暗号化手段を備え、第２の暗号化手段は、第１の暗号化データに代えて、第３の暗号化データに外部認証データを付加して第２の暗号鍵で暗号化して第２の

暗号化データを生成する電子文書の改竄防止システムである。

【００２８】本発明はこのような手段を設けたので、請求項１の発明と同様な効果が得られる他、認証データに第２の当事者の暗号鍵による暗号化を加え、この電子文書を第１の当事者、第２の当事者及び外部認証者の三者の認証になる電子傾斜区処とすることができる。

【００２９】次に、請求項４に対応する発明は、請求項１～３に対応する発明において、第２の暗号化データを、第２の暗号鍵とは異なる第４の暗号鍵で暗号化して第４の暗号化データを生成し、認証データとする第４の暗号化手段をを備える電子文書の改竄防止システムである。

【００３０】本発明はこのような手段を設けたので、例えば認証データ作成から長期間をへて、技術の進歩でその暗号が解読される可能性が生じたような場合でも、請求項１～３のうち何れか１項記載の電子文書の改竄防止システムにて生成された第２の暗号化データについて、再度の暗号化による外部認証者の再認証を行うことができ、電子文書の改竄に対する防御性を維持することができる。

【００３１】次に、請求項５に対応する発明は、認証対象の電子文書に対応する認証データから第２の暗号化データを取り出し、これを第２の暗号鍵に対応する第２の公開鍵で復号化する第２の復号化手段と、第２の復号化手段により復号化されたデータから第１の暗号化データを取り出し、これを第１の暗号鍵に対応する第１の公開鍵で復号化する第１の復号化手段と、電子文書から特徴を抽出して照会用特徴データを生成する特徴抽出手段と、第１の復号化手段により復号化されたデータから特徴データを取り出し、照会用特徴データと照合する照合手段とを備えた認証文書確認システムである。

【００３２】本発明はこのような手段を設けたので、本来紙文書の特徴である証拠能力が付与された電子文書について、その認証事実及び認証日を確認するとともに、真の意味での文書の電子化を推進するのに貢献できるシステムを提供することができる。これにより、ひいては、文書の保管場所の削減、文書の検索の効率化、本紙の文書の遠方への即時配達等を実現することができる。

【００３３】次に、請求項６に対応する発明は、請求項５に対応する発明において、第２の復号化手段により復号化されたデータから第３の暗号化データを取り出し、これを第３の暗号鍵に対応する第３の公開鍵で復号化する第３の復号化手段を設け、第１の復号化手段は第３の復号化手段により復号化されたデータから第１の暗号化データを取り出し、これを第１の暗号鍵に対応する第１の公開鍵で復号化する認証文書確認システムである。

【００３４】本発明はこのような手段を設けたので、第２の当事者を交えた電子契約書についても、請求項５の発明と同様な効果を得ることができる。

【００３５】次に、請求項７に対応する発明は、特徴抽出対象データを１単位づつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第１の合計値列とする第１列生成手段と、この１単位づつ読み出した値に対して規定の単位数だけ隔てた関係となる１単位づつ読み出した値を加算し、この加算した値に対して関係となる１単位づつ読み出した値を加算し、この加算を繰り返し、合計加算回数として規定の単位数回の加算を行って得られる合計値を順次並べて第２の合計値列とする第２列生成手段と、第１の合計値列及び第２の合計値列を特徴データとして出力する手段とを備えた特徴抽出装置である。

【００３６】本発明はこのような手段を設けたので、こうして得られた特徴データのみからではもとの電子文書を再現できず、その改変を行えばその旨を検出でき、かつ、もとの電子文書を大幅にデータ圧縮した特徴データを生成することができる。

【００３７】次に、請求項８に対応する発明は、請求項７に対応する発明において、第１の合計値列を１単位づつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第３の合計値列とする第３列生成手段と、第２の合計値列を１単位づつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第４の合計値列とする第４列生成手段と、第３の合計値列及び第４の合計値列を特徴データとして出力する手段とを備えた特徴抽出装置である。

【００３８】本発明はこのような手段を設けたので、請求項７の発明と同様な効果が得られる他、特徴データをより圧縮することができる。

【００３９】次に、請求項９に対応する発明は、指紋読取手段と、指紋読取手段で読み取った指紋データから特徴抽出を行い指紋特徴データを生成する指紋特徴抽出手段と、指紋特徴データ及びパスワードから暗号鍵を生成する暗号鍵生成手段と、指紋特徴データ、パスワード及び乱数値から秘密鍵及び公開鍵を生成する秘密鍵公開鍵生成手段と、暗号鍵で暗号鍵自身と秘密鍵をそれぞれ暗号化する暗号化手段と、暗号化手段で暗号化したデータ、指紋データ及びパスワードを本人認証データとする手段とを備えた本人認証データ生成システムである。

【００４０】本発明はこのような手段を設けたので、指紋等を用いて有効な本人認証データを作成することができる。なお、本システムで作成した本人認証データは、例えば文書改竄防止システムや認証文書確認システムの起動時の本人確認用のデータとすることができる。

【００４１】次に、請求項１０に対応する発明は、請求項９に記載された本人認証データ生成システムで生成した本人認証データ中のパスワードと、入力されたパスワードとを照合するパスワード照合手段と、指紋読取手段と、両パスワードが一致した場合には、指紋読取手段で指紋読み取りを行い、本人認証データ中の指紋データ

と、指紋読取手段にて読み取られた指紋データとを照合する指紋照合手段と、指紋照合が一致した場合には、本人認証データ中の指紋データから特徴抽出を行い指紋特徴データを生成する指紋特徴抽出手段と、指紋特徴抽出手段にて生成された指紋特徴データ及びパスワードから暗号鍵を生成する暗号鍵生成手段と、この生成された暗号鍵により本人認証データ内の暗号化された暗号鍵を復号して、生成された暗号鍵と復号した暗号鍵とを照合する暗号鍵照合手段と、暗号鍵照合が一致した場合には、この暗号鍵を用いて本人認証データ中の暗号化した秘密鍵を復号する秘密鍵復号手段とを備えた秘密鍵復号システムである。

【００４２】本発明はこのような手段を設けたので、例えば文書改竄防止システムや認証文書確認システムの起動時に本人を高い確実性をもって確認することができる。

【００４３】次に、請求項１１に対応する発明は、指紋読取手段と、指紋読取手段から読み取られる指紋データの境界を検出する境界検出手段と、境界検出手段により境界検出された指紋データをエンボス処理するエンボス手段と、エンボス手段によりエンボス処理された指紋データを輪郭トレースする輪郭トレース手段とを備えた指紋データ抽出装置である。

【００４４】本発明はこのような手段を設けたので、計算機で扱うことのできるデジタルデータとして指紋を抽出することができる。

【００４５】次に、請求項１２に対応する発明は、請求項１１に記載された指紋データ抽出装置から抽出された指紋データから複数の矩形領域を取り出す領域取出手段と、矩形領域のデータと予め登録した複数パターンとを比較し、何れかのパターンとマッチングするか否かを判定するパターンマッチング手段と、マッチングしたパターンに対応する数値を数列として並べ、当該数列を指紋特徴データとする手段とを備えた指紋特徴抽出装置である。

【００４６】本発明はこのような手段を設けたので、効果的に指紋データから指紋特徴データを抽出することができる。

【００４７】次に、請求項１３に対応する発明は、請求項１の発明を方法発明としたものであり、請求項１の発明と同様な効果を奏する。

【００４８】次に、請求項１４に対応する発明は、請求項２の発明を方法発明としたものであり、請求項２の発明と同様な効果を奏する。

【００４９】次に、請求項１５に対応する発明は、請求項３の発明を方法発明としたものであり、請求項３の発明と同様な効果を奏する。

【００５０】次に、請求項１６に対応する発明は、請求項１，２又は３記載の電子文書の改竄防止システムにて生成された認証データから第２の暗号化データを取出し、これを第２の秘密鍵に対応する第２の公開鍵で復号化する第２の復号化ステップと、第２の復号化ステップにより復号化されたデータから第１の暗号化データを取出し、これを第１の秘密鍵に対応する第１の公開鍵で復号化する第１の復号化ステップと、電子文書から特徴を抽出して照合用特徴データを生成する特徴抽出ステップと、第１の復号化ステップにより復号化されたデータから特徴データを取出し、これを照合用特徴データと照合する照合ステップと、照合ステップによる照合結果と、第２の復号化手段により復号化されたデータから取り出された外部認証データによって、外部認証者による認証の事実及び認証の日付を出力するステップとを有する認証文書確認方法である。

【００５１】本発明はこのような手段を設けたので、請求項５の発明と同様な効果を奏する。

【００５２】次に、請求項１７に対応する発明は、請求項１の発明を実現させるためのプログラムを格納した記録媒体についての発明であり、このプログラムを実行する計算機は、請求項１の発明における第２の暗号化手段を除いたものと同様な作用効果を奏する。

【００５３】次に、請求項１８に対応する発明は、請求項１，２又は３記載の電子文書の改竄防止システムにて生成された認証データから第２の暗号化データを取出し、これを第２の秘密鍵に対応する第２の公開鍵で復号化する第２の復号化手段と、第２の復号化手段により復号化されたデータから第１の暗号化データを取出し、これを第１の秘密鍵に対応する第１の公開鍵で復号化する第１の復号化手段と、電子文書から特徴を抽出して照合用特徴データを生成する特徴抽出手段と、第１の復号化手段により復号化されたデータから特徴データを取出し、これを照合用特徴データと照合する照合手段と、照合手段による照合結果と、第２の復号化手段により復号化されたデータから取り出された外部認証データによって、外部認証者による認証の事実及び認証の日付を出力する手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００５４】本発明はこのような手段を設けたので、このプログラムを実行する計算機は、請求項５の発明と同様な作用効果を奏する。

【００５５】次に、請求項１９に対応する発明は、請求項１の発明における処理が実行された結果として得られるデータ構造が記録された記録媒体についての発明である。

【００５６】次に、請求項２０に対応する発明は、請求項３の発明における処理が実行された結果として得られるデータ構造が記録された記録媒体についての発明である。

【００５７】次に、請求項２１に対応する発明は、認証付き電子文書から電子文書を取り出して、これに変更を

加えて、新たな電子文書を生成する文書変更手段と、認証付き電子文書から取り出された元の電子文書と新たな電子文書との変更点を抽出して変更箇所データを取得する差分抽出手段と、変更箇所データと新たな電子文書とをそれぞれ変更者認証する変更者認証手段と、変更者認証手段により認証された各データを外部の認証システムに送出するとともに、それぞれを外部認証された認証データを受け取って、受け取った各認証データ及び新たな電子文書に基づいて、認証付き変更箇所データと新たな認証付き電子文書を生成する認証手段とを備えた電子文書の改竄防止システムである。

【００５８】本発明はこのような手段を設けたので、変更された電子文書に新たな認証を付することができるとともに、変更部分のみのデータも認証することができ、変更電子文書の改竄を防止できる。また、外部認証を得ているので信頼性も高い。

【００５９】次に、請求項２２に対応する発明は、請求項２１に対応する発明において、変更者認証手段は、変更箇所データ及び又は新たな電子文書から特徴抽出して特徴データを出力する特徴抽出手段と、特徴データを、新たな電子文書を生成した変更者の暗号化鍵で暗号化して出力する暗号化手段とを備えた電子文書の改竄防止システムである。

【００６０】本発明はこのような手段を設けたので、変更箇所データ及び又は新たな電子文書そのものでなく、その特徴データを暗号化したものを認証データとするために認証元の特徴を残しつつ安全性を高めることができる。さらに認証データのデータ量を少なくできる。

【００６１】次に、請求項２３に対応する発明は、請求項２２に対応する発明において、変更者認証手段は、暗号化手段から出力されかつ新たな電子文書に対応する暗号化特徴データと、元の認証付き電子文書から取り出された以前の認証データとを結合して出力する結合手段を備えた電子文書の改竄防止システムである。

【００６２】本発明はこのような手段を設けたので、変更後の新たな電子文書に付する認証データに以前の認証データを含めることができ、変更毎の履歴とすることができる。また、各回の認証データを保持できる。

【００６３】次に、請求項２４に対応する発明は、請求項２２に対応する発明において、変更者認証手段は、特徴抽出手段により特徴抽出された特徴データと、元の認証付き電子文書から取り出された以前の認証データとを結合して出力する結合手段を備え、暗号化手段の暗号化対象として、結合手段からの出力データを特徴データに代えて入力する電子文書の改竄防止システムである。

【００６４】本発明はこのような手段を設けたので、請求項２３に対応する発明と同様な効果を他の手法で実現できる。

【００６５】次に、請求項２５に対応する発明は、請求項２１乃至２４のうち何れか１項に記載された認証手段により生成された認証付き変更箇所データと認証付き電子文書とを含む変更済電子文書から、認証付き変更箇所データ及び認証付き電子文書を取り出す分離手段と、請求項２１乃至２４のうち何れか１項に記載された文書変更手段、差分抽出手段、変更者認証手段及び認証手段と、認証手段により生成された新たな認証付き変更箇所データ及び新たな認証付き電子文書と、分離手段で分離された元の認証付き変更箇所データとに基づき、新たな変更済電子文書を生成する結合手段とを備えた電子文書の改竄防止システムである。

【００６６】本発明はこのような手段を設けたので、複数回の変更があっても変更後の電子文書を増やすことなく、かつ各変更毎の認証データを保持できる変更済電子文書を作成することができる。

【００６７】次に、請求項２６に対応する発明は、請求項２１乃至２４のうち何れか１項に記載された変更者認証手段により認証された各データを受け取る受入手段と、各データそれぞれに、少なくとも日付データ及び認証実行識別情報を結合する結合手段と、この結合手段により結合された各データを外部認証機関の暗号鍵によって暗号化して、外部認証された認証データを作成する暗号化手段とを備えた電子文書の外部認証システムである。

【００６８】本発明はこのような手段を設けたので、変更電子文書の確実かつ安全な認証を行うことができる。

【００６９】次に、請求項２７に対応する発明は、請求項２６に記載の外部認証システムにより外部認証された認証データを、外部認証機関の復号鍵で復号する復号化手段と、復号化手段により復号された認証データから、日付データ及び認証実行識別情報を取り出すデータ取出手段とを備えた認証文書確認システムである。

【００７０】本発明はこのような手段を設けたので、認証日付及び外部認証機関における認証情報（認証実行ＩＤ等）を取得することができる。

【００７１】次に、請求項２８に対応する発明は、請求項２７に対応する発明において、請求項２６に記載の外部認証システムにより外部認証された認証データが請求項２３に対応しかつ電子文書に対応するものである場合に、復号化手段により復号された認証データから、以前の認証データを取り出す認証データ取出手段を備えた認証文書確認システムである。

【００７２】本発明はこのような手段を設けたので、複数回の変更認証がなされている場合、各回の認証データひいては外部認証情報を取り出すことができる。

【００７３】次に、請求項２９に対応する発明は、請求項２８に対応する発明において、復号化手段により復号された認証データのうち、請求項２２の暗号化手段で暗号化された暗号データが入力されるとともに、当該暗号データを変更者の復号鍵で復号して特徴データを取り出す第２の復号化手段と、請求項２１の文書変更手段で得

られた新たな電子文書から特徴抽出して比較用特徴データを出力する特徴抽出手段と、第２の復号化手段で得られた特徴データと、特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えた認証文書確認システムである。

【００７４】本発明はこのような手段を設けたので、電子文書が真正なものであるかを確認することができる。

【００７５】次に、請求項３０に対応する発明は、請求項２７に対応する発明において、請求項２６に記載の外部認証システムにより外部認証された認証データが請求項２４に対応しかつ電子文書に対応するものである場合に、復号化手段により復号された認証データを変更者の復号鍵で復号する第２の復号化手段と、第２の復号化手段で復号化された認証データから、以前の認証データを取り出す認証データ取出手段とを備えた認証文書確認システムである。

【００７６】本発明はこのような手段を設けたので、請求項２８に対応する発明と同様な効果を他の手法で得ることができる。

【００７７】次に、請求項３１に対応する発明は、請求項３０に対応する発明において、第２の復号化手段で復号化された認証データから、特徴データを取り出す分離手段と、請求項２１の文書変更手段で得られた新たな電子文書から特徴抽出して比較用特徴データを出力する特徴抽出手段と、分離手段で得られた特徴データと、特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えた認証文書確認システムである。

【００７８】本発明はこのような手段を設けたので、請求項２９に対応する発明と同様な効果を他の手法で得ることができる。

【００７９】次に、請求項３２に対応する発明は、請求項２７に対応する発明において、請求項２６に記載の外部認証システムにより外部認証された認証データが請求項２２に対応しかつ変更箇所データに対応するものである場合に、復号化された認証データのうち、請求項２２の暗号化手段で暗号化された暗号データが入力されるとともに、当該暗号データを変更者の復号鍵で復号して特徴データを取り出す第２の復号化手段と、請求項２１の差分抽出手段で得られた変更箇所データから特徴抽出して比較用特徴データを出力する特徴抽出手段と、第２の復号化手段で得られた特徴データと、特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えた認証文書確認システムである。

【００８０】本発明はこのような手段を設けたので、各回における変更箇所データの正当性が確認でき、ひいては電子文書が真正なものであるかを確認できる。

【００８１】次に、請求項３３に対応する発明は、請求項２５に記載された電子文書の改竄防止システムにより作成された変更済電子文書の変更部分についての認証確認を行うシステムであって、請求項２８又は３０の認証文書確認システムと、請求項３２の認証文書確認システムとを備えるとともに、複数回の変更を受けた最終的な変更済電子文書における認証付き電子文書から、最終変更回に関する認証データを取り出し、まずこれを請求項２６に記載の外部認証システムにより外部認証された認証データとして請求項２８又は３０の認証文書確認システムに入力し、最終変更回以外の各回については、請求項２８又は３０の認証文書確認システムから出力される以前の認証データを、請求項２６に記載の外部認証システムにより外部認証された認証データとして、順次、請求項２８又は３０の認証文書確認システムに入力し、また、複数回の変更を受けた最終的な変更済電子文書から、各回の認証付き変更箇所データを取り出し、この認証付き変更箇所データを変更箇所データ及び請求項２６に記載の外部認証システムにより外部認証された認証データに分離して、請求項３２の認証文書確認システムに入力し、請求項２８又は３０の認証文書確認システムから得られた日付データ及び認証実行識別情報と、請求項３２の認証文書確認システムから得られた日付データ及び認証実行識別情報とを各変更回毎に照合する変更済電子文書の認証確認システムである。

【００８２】本発明はこのような手段を設けたので、変更済電子文書の真実性を確認でき、証拠としての使用を可能とする。

【００８３】次に、請求項３４に対応する発明は、請求項３３に対応する発明において、請求項２９又は３１の認証文書確認システムを備えるとともに、最終的な変更済電子文書に包含される認証付き電子文書から取り出された認証データ及び新たな電子文書を、請求項２８又は３０の認証文書確認システムに代えて請求項２９又は３１の認証文書確認システムに入力する変更済電子文書の認証確認システムである。

【００８４】本発明はこのような手段を設けたので、より一層電子文書の証拠能力を高めることができる。

【００８５】次に、請求項３５に対応する発明は、請求項２１に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【００８６】この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項２１の電子文書の改竄防止システムとして機能する。

【００８７】次に、請求項３６に対応する発明は、請求項２２に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【００８８】この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項２２の電子文書の改竄防止システムとして機能する。

【００８９】次に、請求項３７に対応する発明は、請求項２７に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【００９０】この記録媒体から読み出されたプログラム

により制御されるコンピュータは、請求項２７の認証文書確認システム電子文書の改竄防止システムとして機能する。

【００９１】

【発明の実施の形態】次に、本発明の実施の形態について説明する。

【００９２】［第１～第１３の実施形態についての説明］図１は本発明の各実施形態における電子文書の改竄防止システム及び方法の全体的な構成を示す図である。

【００９３】公衆回線や専用回線を用いたネットワーク１００が構成され、当該ネットワークに文書認証システム１０１や外部認証機関９９の外部認証システム１０２、認証文書確認システム１０３が接続されている。

【００９４】文書認証システム１０１は、認証対象となる電子文書に関する当該システム使用者作成の所定情報（使用者の鍵で暗号化したことによる一種の使用者認証を含む）をネットワーク１００を介して外部認証システム１０２に送付し、この所定情報を元に外部認証システム１０２で作成された認証のための情報の返信を受け認証電子文書を作成する。また、後の実施形態でも説明するが、複数の文書認証システム１０１でそれぞれ異なるシステム使用者に加工（暗号化や認証情報付加等であり、各使用者による実質的な認証になっている）された所定情報が外部認証システム１０２に送付される場合もある。

【００９５】一方、認証文書確認システム１０３は、上記認証電子文書の正当性を確認するためのシステムであり、ネットワーク１００を介し文書認証システム１０１等から確認対象の認証電子文書を受信する。

【００９６】文書認証システム１０１、外部認証システム１０２及び認証文書確認システム１０３は、ワークステーションやパーソナルコンピュータ等の計算機に表示装置、入力装置、あるいは例えば指紋読取り機等を付加したものであり、基本的にはその動作プログラムが相違することで異なる各機能を実現する。したがって、図１に示すように、例えば文書認証システム１０１と認証文書確認システム１０３とが同一の計算機上に構成される場合もある。

【００９７】さらに、文書認証システム１０１と外部認証システム１０２とを同一計算機、あるいはＬＡＮ等で接続される計算機上に構成させ、外部認証機関において認証作業のすべてを行うようにすることも可能である。

【００９８】本発明にかかわる電子文書の改竄防止システム及び方法は、これらの文書認証システム１０１、外部認証システム１０２及び認証文書確認システム１０３を適宜組み合わせ、あるいはその一部機能を適宜組み合わせてなるものである。

【００９９】また、上記場合は、ネットワークを介した情報の瞬時転送を前提とした場合を説明しているが、図１に示すように、フロッピーディスク等の記録媒体９７，９８を介して文書認証システム１０１～外部認証システム１０２間、あるいは文書認証システム１０１～認証文書確認システム１０３間で必要情報（所定情報や電子文書）の交換を行うことも可能である。

【０１００】全体的には以上のシステム構成を有する電子文書の改竄防止システム及び方法について、その各実施形態を以下に説明する。

【０１０１】（第１の実施の形態）本実施形態は改竄を防止できる電子文書の作成システム及び方法に関するものである。

【０１０２】図２は本発明の第１の実施の形態に係る電子文書の改竄防止システムに適用される文書認証システムのハードウエア構成例を示すブロック図である。

【０１０３】文書認証システムは、計算機１１０に、表示装置１１１、入力装置１１２、印刷装置１１３、外部記憶装置１１４、指紋読取り機６４、スキャナ１１５が接続されてなっている。

【０１０４】計算機１１０においては、ＣＰＵバス１１６にＣＰＵ１１７、ＲＯＭ１１８、ＲＡＭ１１９が接続され、さらに、ＣＰＵバス１１６に接続される各インターフェース手段１２０，１２１，１２２，１２３，１２４，１２５，１２６，１２７を介してそれぞれハードディスク装置１２８、通信装置１２１、表示装置１１１、入力装置１１２、印刷装置１１３、外部記憶装置１１４、指紋読取り機６４、スキャナ１１５が接続されている。

【０１０５】ＲＯＭ１１８は、コンピュータ１１０を起動しオペレーティングシステム（ＯＳ）等を立ち上げるのに用いられるブート処理プログラム等が格納されている。

【０１０６】また、ハードディスク装置１２８には、プログラム格納部１３０及びデータ格納部１３１が設けられている。プログラム格納部１３０は、ＯＳや、文書認証システム１０１を実現するプログラム等を格納し、データ格納部１３１は、電子文書、認証付き電子文書、その他各種情報を格納する。

【０１０７】ＲＡＭ１１９は、いわゆる主記憶に使用される。すなわち、ＣＰＵ１１７による各種処理のための作業領域１３２を備え、またＣＰＵ１１７を制御する文書認証プログラム１３３を格納している。

【０１０８】この文書認証プログラム１３３は、ハードディスク装置１２８のプログラム格納部１３０から呼び出され、ＲＡＭ１１９内に格納されるものである。

【０１０９】ＣＰＵ１１７は、ＲＡＭ１１９内の文書認証プログラム１３３に従って各部を制御し、文書認証システム１０１を実現する。つまり、ＲＡＭ１１９（特に文書認証プログラム１３３）やハードディスク装置１２８等のソフトウエア資源とＣＰＵ１１７等の図２のハードウエア資源とが結合して文書認証システム１０１の各機能実現手段が構成される。本実施形態及び以下の各実

施形態における処理説明図や流れ図等に表現される各手段（各処理）あるいは図示しない各手段（各処理）は、このような機能実現手段であり、主として文書認証プログラム１３３に従うＣＰＵ１１７の動作によるものである。

【０１１０】通信装置１２９は、外部認証システム１０２と間あるいは認証文書確認システム１０３と間の通信を行うものである。電子文書や各種情報の授受が行われる。

【０１１１】外部記憶装置１１４は、電子文書、認証付き電子文書、その他各種情報を可搬な記録媒体に格納し、特に認証付き電子文書の保存、送付等を便利かつ容易にするものである。外部記憶装置１１４としては、例えばフロッピーディスク装置、光磁気ディスク装置（ＭＯ）、ＣＤ－Ｒ、ＣＤ－Ｒ／ＷあるいはＤＶＤ等が用いられる。

【０１１２】指紋読取り機６４は、人間の指紋情報を読み取る装置である。システム使用者の認証や暗号情報作成等のために用いられる。

【０１１３】スキャナ１１５は、印鑑等の図形をイメージ情報として読み取る装置である。

【０１１４】次に外部認証システムのハードウエア構成について説明する。

【０１１５】図３は本実施形態の電子文書の改竄防止システムに適用される外部認証システムのハードウエア構成例を示すブロック図であり、図２と同一部分には同一符号を付してその説明を省略する。

【０１１６】外部認証システム１０２は、文書認証システム１０１と同様な計算機システムから構成される。文書認証システム１０１との相違点は、ハードディスク装置１２８のプログラム格納部１３０に格納される動作プログラムである。この動作プログラムが呼び出され、ＲＡＭ１１９内に外部認証プログラム１３４として格納される。ＣＰＵ１１７は、この外部認証プログラム１３４に従って各部を制御し、外部認証システム１０２が実現される。また、ソフトウエア資源（特に外部認証プログラム１３４）とハードウエア資源とが結合して機能実現手段が構成される点も文書認証システム１０１の場合と同様である。

【０１１７】次に、図４を用いて電子文書の改竄防止システムの各機能について説明する。図４は本実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図である。

【０１１８】この電子文書の改竄防止システムは、文書認証システム１０１と外部認証システム１０２とから構成されている。

【０１１９】文書認証システム１０１は、認証すべき電子文書１から特徴データ３Ｄを抽出し暗号化するとともに、この暗号化データ６について認証を与える外部認証機関の外部認証システム１０２から合成データ１０を受け取り、これを上記電子文書１に付与して認証付き電子文書１２を作成する。

【０１２０】このために文書認証システム１０１は、見出し３Ｈの取出編集手段（図示せず）と、電子文書１から特徴抽出を行って特徴データ３Ｄを生成する特徴抽出手段２と、特徴データ３Ｄを第１の秘密鍵４（＃１）（以下、複数存在し得る同種類の構成やデータには、場合により＃１，＃２，．．あるいは第１の、第２の、．．と記して区別する）にて暗号化し暗号化データ６Ｄ（＃１）を生成する暗号化手段６と、見出し３Ｈと暗号化データ６Ｄとを結合する手段（図示せず）と、結合された見出し付き暗号化データ６を外部認証システム１０２に送信する通信手段（図示せず）と、外部認証システム１０２から受け取った合成データ１１を電子文書１に付与して認証付き電子文書１２を作成し電子媒体に保存する手段（図示せず）を備えている。

【０１２１】一方、外部認証システム１０２は、文書認証システム１０１から受け取った見出し付き暗号データ６を分離手段（図示せず）で分離し、このうちの暗号データ７Ｄに外部認証データ７Ａ（＃１）を付与しこれを暗号化手段９を用いて第２の秘密鍵８（＃２）にて暗号化した後、この暗号データ１０Ｄと見出し１０Ｈからなる合成データ１０を結合手段（図示せず）で結合して通信手段（図示せず）により文書認証システム１０１に送信する。

【０１２２】なお、本実施形態では、各データの暗号化方式として秘密鍵と公開鍵を使用したＲＳＡ方式が用いられるが、他の暗号化方式（ＤＥＳ方式等）を用いてもよい。

【０１２３】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図４及び図５を用いて説明する。

【０１２４】図５は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０１２５】まず、文書認証システム１０１において電子文書１のデータが読み込まれ（Ｓ１）、その文書データから文書タイトルや日付等の見出し３Ｈのデータに使用できる部分が取り出され、更に補足説明を追加する為に編集が行される。こうして見出し３が作成される（Ｓ２）。なお、見出し３には例えば第７実施形態で説明する文書作成者の電子印鑑や電子署名等も含まれる。

【０１２６】次に、特徴抽出手段２により電子文書１から特徴が抽出され特徴データ３Ｄが作成される（Ｓ３）。ここで、特徴データ３Ｄは、例えば電子文書の１ビットが変化しても異なった値となるような電子文書自体の特徴を示すデータである。一方、見出し３Ｈは特徴データ３Ｄがどの電子文書のものであるかを分かるようにする為に追加されるデータである。見出し３Ｈと特徴データ３Ｄは合成データ（見出し付き特徴データ３）として対応が取られるようにする。

25

【０１２７】次に、暗号化手段５により秘密鍵４（＃１）が用いられ、特徴データ３Ｄが暗号化され第１の暗号データ６Ｄが生成される（Ｓ４）。なお、第１の秘密鍵４は電子文書１の作成者が保有する秘密鍵であり、他人には知らせないようにしたものである。

【０１２８】次に、見出し６Ｈと暗号データ６Ｄを結合し見出し付き暗号データ６として対応が取られる（Ｓ５）。なお、見出し６Ｈは見出し３Ｈと同じものである。このようにしてできた見出し付き暗号データ６は外部認証機関の外部認証システム１０２に送信される（Ｓ６）。なお、この送信は、本実施形態では公衆回線や専用回線を介し、ネットワーク１００に伝送されるが、例えばフロッピーディスク等の電子媒体に記録して郵送等してもよい。

【０１２９】一方、外部認証機関では、文書認証システム１０１からの見出し付き暗号データ６が受信される（Ｓ７）。

【０１３０】外部認証システム１０２では見出し付き暗号データ６が見出し７Ｈと暗号データ７Ｄに分解される（Ｓ８）。このうちの暗号データ７Ｄに外部認証データ７Ａが結合される（Ｓ９）。この外部認証データ７Ａは、文書認証システム１０１が認証を要求してきたデータについて第三者である外部認証機関が認証したことを示す情報であり、認証した日付データが含まれる。

【０１３１】次に、暗号化手段９により第１の暗号データ７Ｄ（＃１）と外部認証データ７Ａ（＃１）が纏められ、秘密鍵８で暗号化される（Ｓ１０）。こうして第２の暗号データ１０Ｄ＃２が生成される。これにより第２の暗号データ１０Ｄ（＃２）は作成者の秘密鍵４と外部認証機関の秘密鍵８で二重に鍵が掛けられたデータとなり、かつそれぞれ独自のデータが含まれる。

【０１３２】さらに、第２の暗号データ１０Ｄは見出し１０Ｈと合成されて合成データ１０となり、その取り扱いが容易に形になる（Ｓ１１）。なお、見出し１０Ｈは見出し３Ｈと同じ内容である。そして、合成データ１０は外部認証システム１０２から第三者認証を要求する作成者の文書認証システム１０１にネットワーク１００を介して返信される（Ｓ１２）。

【０１３３】文書認証システム１０１では、合成データ１０が合成データ１１として受け取られる（Ｓ１３）。そして、この合成データ１１は電子文書１と合成されて認証付き電子文書１２が生成される。このような結合をすればデータ取り扱いが容易になる。生成された認証付き電子文書１２は任意の場所の電子媒体に保管することができ、何れの場所に保管されても認証機能を発揮することになる。なお、ここでいう結合というのは、単に同一の記録媒体に合成データ１１と電子文書１とを記録する場合や、両者の関連付けを示す他のデータを作成する場合等、様々な場合を含むものである。この結合する手段は、請求項における電子文書の認証データとする手段の一例でもある。

26

【０１３４】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、本人により電子署名された文書を外部認証機関が認証する手順を踏むことにより、外部認証機関の認証日付にはまさしく本人が文書を作成していたことが証明される。また、たとえ電子署名がない場合であっても、文書作成者本人の秘密鍵４で特徴データの暗号化がなされ、これに対応する公開鍵で復号化されることになるので、何れにしても文書作成者の作成になる文書であることが認証される。

【０１３５】また、文書本体の改竄を行うと改竄後の文書から抽出されるべき特徴データが変化し、先に認証用に抽出された特徴データ３Ｄと異なるものになることによって元文書の改竄の事実が検出できる。一方、先に認証用に抽出された特徴データ３Ｄは、外部認証機関の認証データ７Ａと共に認証機関の秘密鍵８で暗号化されているので、認証付き電子文書１２に付されている暗号データ１１Ｄの改竄は不可能である。したがって、たとえ本人であっても外部認証後には文書改竄が不可能になる。

【０１３６】これにより裁判の場で文書の正当性が証明できる，証拠能力のある電子文書が生成でき、従来紙で保存していた重要文書や、証拠書類を電子化する事が可能となる。また、従来の紙の文書でも改竄の有無を判定するには高度な技術が必要とされたが、本発明になる電子文書の改竄防止システムでは電子的な手順を踏むだけで改竄の有無を確認できるので、改竄の有無を容易に証明できる。さらに電子化により保管場所が削減されると共に、遠隔地への文書電送が瞬時に行えるようになり、コンピュータによる検索が行えるようになる。こうして、商取引の信用向上、取引の迅速化を図ることができる。

【０１３７】また、本実施形態の文書改竄防止システムでは、文書認証システム１０１や外部認証システム１０２においてそれぞれ電送データの暗号化が行われるので、ネットワーク１００として公衆回線を用いても安全である。

【０１３８】さらに、外部認証機関が認証した外部認証データを元の電子文書に結合して認証付き電子文書１２の形で管理するようにしたので、電子文書を保存する時の扱いが楽になる。

【０１３９】（第２の実施の形態）本実施形態では第１の実施形態で認証した認証付き電子文書１２が真正なものであることを確認し、また外部認証機関の付した認証日付等の認証情報を取り出すシステムについて説明する。

【０１４０】この電子文書の改竄防止システムは、図１に示した認証文書確認システム１０３として構成されるものである。

【０１４１】図６は本発明の第２の実施の形態に係る電

子文書の改竄防止システムに適用される認証文書確認システムのハードウエア構成例を示すブロック図であり、図２と同一部分には同一符号を付してその説明を省略する。

【０１４２】認証文書確認システム１０３は、文書認証システム１０１と同様な計算機システムから構成される。文書認証システム１０１との相違点は、ハードディスク装置１２８のプログラム格納部１３０に格納される動作プログラムである。この動作プログラムが呼び出され、ＲＡＭ１１９内に認証文書確認プログラム１３５として格納される。ＣＰＵ１１７は、この認証文書確認プログラム１３５に従って各部を制御し、認証文書確認システム１０３が実現される。また、ソフトウエア資源（特に認証文書確認プログラム１３５）とハードウエア資源とが結合して機能実現手段が構成される点も文書認証システム１０１の場合と同様である。

【０１４３】次に、図７を用いて電子文書の改竄防止システムの各機能について説明する。図７は本実施形態の電子文書の改竄防止システムに適用される認証文書確認システム１０３の機能構成及び処理流れの一例を示す図であり、図４と同一部分には同一符号を付して説明を省略する。

【０１４４】この認証文書確認システム１０３は、認証付き電子文書１２から取り出した特徴データ１８Ｄと認証付き電子文書１２から合成データ１１を取り除いた電子文書１９から抽出される特徴データ２１とを照合し、電子文書の同一性を行うとともに、認証データ（暗号データ１１Ｄ）より取り出された外部認証データ１５Ａから外部認証機関９９による認証の事実及びその認証日付を確認する。

【０１４５】このために認証文書確認システム１０３には、外部記憶装置１１４やハードディスク装置１２８に格納された認証付き電子文書１２から見出し１１Ｈ及び暗号データ１１Ｄを取り出す手段（図示せず）と、暗号データ１１Ｄを外部認証システム１０２の第２の公開鍵１３（＃２）により復号化する復号化手段１４と、この復号化により得られたデータのうちの外部認証データ１５Ａ（＃１）により日付認証１５Ａ－Ｄ及び外部認証機関９９の認証確認を行う手段（図示せず）と、復号化手段１４で復号化されたデータのうちの暗号データ１５Ｄを文書認証システム１０１の第１の公開鍵１６（＃１）で復号化する復号化手段１７とが設けられている。さらに、認証データを取り除いた電子文書１９から特徴データ２１を取り出す特徴抽出手段２０と、この特徴データ２１と，復号化手段１７で復号化された見出し付き特徴データ１８から取り出した特徴データ１８Ｄとを照合し、電子文書１９が電子文書１と同一であるか否かの同一性判定２２－Ｊを行う照合手段とが設けられている。

【０１４６】本実施形態では、秘密鍵と公開鍵を使用した暗号としてはＲＳＡ方式が用いられるが、他の暗号化方式（ＤＥＳ方式等）を用いてもよい。なお、図７に示す認証文書確認システム１０３は電子文書１の作成者のシステムでも第三者のシステムでもかまわない。

【０１４７】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図７及び図８を用いて説明する。

【０１４８】図８は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０１４９】まず、外部記憶装置１１４、ハードディスク装置１２８から、あるいはネットワーク１００を介して電子文書１２が読み込まれ（Ｔ１）、合成データ１１が取り出される（Ｔ２）。

【０１５０】合成データ１１の中から更に認証データとして機能する第２の暗号データ１１Ｄ（＃２）が取り出される（Ｔ３）。第２の公開鍵１３（＃２）を使用して復号化手段１４で復号が行われる（Ｔ４）。なお、第２の公開鍵１３（＃２）は外部認証機関９９の公開鍵であり、第２の秘密鍵８（＃２）に対応するものである。これによって第１の暗号データ１５Ｄ（＃１）と外部認証データ１５Ａ（＃１）とが取り出される。

【０１５１】次に、見出し付き認証データ１５から暗号データ１５Ｄと外部認証データ１５Ａとが分離される（Ｔ５）。なお、暗号データ１５Ｄは図４の暗号データ６Ｄと内容が同一のものである。また、外部認証データ１５Ａは図４の外部認証データ７Ａと内容が同一のものである。さらに、見出しデータ１５Ｈは図４の見出しデータ３Ｈと内容が同一のものである。

【０１５２】次に、復号された外部認証データ１５Ａから日付認証データ１５Ａ－Ｄが取り出され、外部認証機関が合成データ６の認証を行った日付が確認される（Ｔ６）。

【０１５３】一方、第１の暗号データ１５Ｄ（＃１）は第１の公開鍵１６（＃１）で復号化手段１７によって復号され（Ｔ６）、第１の特徴データ１８Ｄが生成される。第１の公開鍵１６（＃１）は電子文書の作成者の公開鍵であり、第１の秘密鍵４（＃１）に対応するものである。なお、特徴データ１８Ｄは第１の特徴データ３Ｄ（＃１）と内容が同一のものである。

【０１５４】次に、電子文書１２から合成データ１１を除いた電子文書１９が取り出される（Ｔ８）。この電子文書１９は元の電子文書１に対応するものである。さらに、電子文書１９から特徴抽出手段２０により特徴データ２１が取り出される（Ｔ９）。特徴抽出手段２０は特徴抽出手段２と同一の手段であり、電子文書１９の内容が電子文書１と同一であれば同一の特徴データが生成される。

【０１５５】次に、特徴データ１８Ｄと特徴データ２１とが照合手段２２により照合され（Ｔ１０）、照合結果が同一かどうかを示す同一性判定結果２２－Ｊが出力される。同一性判定結果２２－Ｊが判定良（一致）であれ

ば（Ｔ１１）、日付認証データ１５Ａ－Ｄの日付で認証された本人作成の文書である事が証明される。そこで、ステップＴ６で取り出した日付認証と共に文書同一である旨が表示装置１１１に表示される（Ｔ１３）。

【０１５６】一方、同一性判定結果２２－Ｊが判定不良（不一致）であれば（Ｔ１１）、不一致が表示される。

【０１５７】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、暗号化特徴データの付加、本人電子署名及び外部認証機関の認証がなされた電子文書から外部認証機関の外部認証データを取出し、また付加されている特徴データと電子文書本体からの特徴データとを文書作成者の公開鍵１６を用いて照合することで、外部認証機関の認証日付にはまさしく本人が文書を作成していたことが証明される。

【０１５８】電子文書本体の改竄を行うと、電子文書１９から抽出される特徴データ２１が変化することにより、一方、第１の特徴データ３Ｄ，１８Ｄは外部認証機関９９によって改竄を防止される事によって、本人であっても外部認証後には文書改竄が不可能になる。これにより裁判の場で文書の正当性が証明でき、従来紙で保存していた重要文書や、証拠書類を電子化する事が可能となる。

【０１５９】また、従来の紙の文書でも改竄の有無を判定するには高度な技術が必要とされたが、上記照合処理により電子文書の改竄防止システムでは容易に改竄の有無を証明できる。さらに、電子化により保管場所が削減されると共にネットワークを介して遠隔地への電送が瞬時に行い得る。したがって、さらに、コンピュータによる検索も可能である。

【０１６０】また、本実施形態の文書改竄防止システムでは、文書認証システム１０１や外部認証システム１０２においてそれぞれ電送データの暗号化が行われるので、ネットワーク１００として公衆回線を用いても安全である。

【０１６１】さらに、外部認証機関が認証した認証データを元の電子文書に結合する事により、文書を保存する時の扱いが楽になる。

【０１６２】（第３の実施の形態）本実施形態の電子文書の改竄防止システム及び方法では、一旦作成された認証付き電子文書１２に付された合成データ１１にさらに外部認証データを付し、暗号化をかけ直す。これにより改竄防止を強化した電子文書を生成し、認証付き電子文書１２の作成から長期間を経た認証データの秘匿性を維持するものである。

【０１６３】図９は本発明の第３の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４及び図７と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２及び図３に示す文書認証システム１０１及び外部認証システム１０２が用いられており、本実施形態の独自な機能部分は、文書認証プログラム１３３あるいは外部認証プログラム１３４に修正が加えられたことによるものである。

【０１６４】この電子文書の改竄防止システムは、図１に示す文書認証システム１０１と外部認証システム１０２とから構成されている。

【０１６５】文書認証システム１０１は、電子文書１２から合成データ１１を取出し、外部認証システム１０２に送付する手段（図示せず）と、電子文書１２から認証データ１１を取り除いて元の電子文書としたものに外部認証システム１０２から受け取った見出し付き暗号データ２７を認証データとして付加して認証付き電子文書２８とする手段（図示せず）とが加えられる他、第１の実施形態と同様に構成されている。

【０１６６】一方、外部認証システム１０２は、文書認証システム１０１からの合成データ１１に外部認証データ２３Ａを付加するとともに、暗号データ２３Ｄ（暗号データ１１Ｄと同一）と外部認証データ２３Ａとを第３の秘密鍵２４（＃３）で暗号化する暗号化手段２５と、この暗号化された暗号データ２６Ｄと見出し２６Ｈからなる見出し付き暗号データ２６を文書認証システム１０１に送信する手段（図示せず）とが加えられる他、第１の実施形態と同様に構成されている。なお、第３の秘密鍵２４（＃３）は、外部認証機関９９のもう一つの秘密鍵である。

【０１６７】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図９及び図１０を用いて説明する。

【０１６８】図１０は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０１６９】まず、文書認証システム１０１において、外部記憶装置１１４、ハードディスク装置１２８から、あるいはネットワーク１００を介して電子文書１２が読み込まれ（Ｕ１）、認証データである合成データ１１が取り出される（Ｕ２）。この合成データ１１が外部認証機関９９の外部認証システム１０２にネットワーク１００を介して送信される（Ｕ３）。

【０１７０】）。

【０１７１】次に、外部認証システム１０２において、ステップＵ３で送信された合成データ１１（認証データ）が受信される。次に受け取った合成データ１１が見出し２３Ｄと暗号データ２３Ｄに分離される（Ｕ５）。ここで見出し付き認証データ２３に外部認証データ２３Ａが追加される。なお、外部認証データ２３Ａは、第１の実施形態の外部認証データ７Ａと同様なものであり、認証日等の情報が含まれる。

【０１７２】次に、暗合データ２３Ｄと外部認証データ２３Ａが結合され（Ｕ６）、この結合データが秘密鍵２４（＃３）にて暗号化され暗号データ２６Ｄが生成される（Ｕ７）。なお、この秘密鍵２４は、外部認証機関９

９の秘密鍵であり、例えばＲＳＡ方式に対応するものである。

【０１７３】次に、見出し２６Ｈと暗合データ２６Ｄとが結合されてなる認証データである暗号データ２６が生成され（Ｕ８）、当該データ２６が文書認証システム１０１にネットワーク１００を介して送信される（Ｕ９）。

【０１７４】外部認証機関９９から送信された暗号データ２６が文書認証システム１０１により受信される（Ｕ１０）。これが見出し付き暗号データ２７とされ、電子文書１２から暗号データ１１を取り除いた元の電子文書に合成されて認証付き電子文書２８が生成される（Ｕ１１）。こうして改竄防止が強化された電子文書が生成されることになる。なお、電子文書２８は外部記憶装置１１４やハードディスク装置１２８、その他の任意の場所の電子媒体に保管することができる。

【０１７５】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、電子文書１２から取り出した合成データ１１に再度外部認証機関９９の認証を与え、暗号をかけ直して認証付き電子文書２８を生成するようにしたので、改竄防止を強化した文書２８を作成することができる。

【０１７６】したがって、暗号技術の進歩により、最初の暗号が解読される恐れがある年数を経過する前に、更に新しい暗号により文書１の改竄防止を強化することでき、たとえ長期間の電子文書保管を行っても、裁判の場で文書の正当性が証明できるようになる。

【０１７７】なお、本実施形態では、電子文書１２の如く１度の認証の電子文書を再認証する場合を説明したが、本実施形態の手法を用いて電子文書２８をさらに再認証するようにしてもよい。このように再認証を繰り返し認証の回数を重ねる事によって、電子文書１の保管年限が延長でき、事実上無限長とすることができる。したがって、本実施形態では、公開鍵方式（ＲＳＡ）の暗号方式で際認証する場合を説明したが、その時々に開発された最も解読困難な暗号方式で適宜再認証（再暗号化）することが適当である。

【０１７８】（第４の実施の形態）本実施形態では第３の実施形態で再認証し改竄防止を強化した認証付き電子文書２８が真正なものであることを確認し、また外部認証機関の付した各認証日付等の認証情報を取り出すシステムについて説明する。

【０１７９】図１１は本発明の第４の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７及び図９と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図６に示す認証文書認証システム１０３が用いられており、本実施形態の独自な機能部分は、認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０１８０】この電子文書の改竄防止システムは、図１に示した認証文書確認システム１０３として構成されるものである。

【０１８１】認証文書確認システム１０３は、認証付き電子文書２８から取り出した認証データについて３回の復号処理を施して特徴データ１８Ｄを取出し、電子文書１９から取り出した特徴データ２１との照合を行うとともに、その過程で、外部認証機関９９による２回の認証についてそれぞれの認証日付及び外部認証の旨の確認を行うようになっている。

【０１８２】このために、認証文書確認システム１０３には、認証付き電子文書２８から見出し付き暗号データ２７を取り出す手段（図示せず）と、外部認証機関９９の公開鍵２９（＃３）により暗号データ２７Ｄを復号化する復号化手段３０と、復号化された外部認証データ３１Ａから外部認証機関９９の認証確認を行い日付認証３１Ａ－Ｄを取り出す手段（図示せず）とが設けられる他、図７に示す第２の実施形態と同様に構成されている。なお、復号化手段１４が復号するデータは、暗号データ３１Ｄである。

【０１８３】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図１１及び図１２を用いて説明する。

【０１８４】図１２は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０１８５】まず、認証文書確認システム１０３において、外部記憶装置１１４、ハードディスク装置１２８から、あるいはネットワーク１００を介して認証付きの電子文書２８が読み込まれる（Ｖ１）。次に、電子文書２８から認証データである見出し付き暗号データ２７が取出される（Ｖ２）。さらに見出し付き暗号データ２７から暗号データ２７Ｄが分離される（Ｖ３）。復号化手段３０により、この分離された暗号データ２７Ｄが外部認証機関の公開鍵２９（＃３）で復号化される（Ｖ４）。これによって、暗号データ３１Ｄと第２の外部認証データ３１Ａの合成データが生成される。ここで認証データに改竄がなければ、暗号データ３１Ｄは、暗号データ１１Ｄ又は１０Ｄと同じものであり、第２の外部認証データ３１Ａは、外部認証データ２３Ａと同じものである。

【０１８６】次に、暗号データ３１Ｄと第２の外部認証データ３１Ａとが分離される（Ｖ５）。さらに、外部認証データ３１Ａから日付認証３１Ａ－Ｄが取出され、この２回目の外部認証機関９９の認証が確認される（Ｖ６）。一方、暗号データ３１Ｄは外部認証機関９９の公開鍵１３（＃２）を使用して復号化手段１４により復号され、暗号データ１５Ｄと外部認証データ１５Ａの合成データが生成される（Ｖ７）。ここで認証データに改竄がなければ、暗号データ１５Ｄは、暗号データ６Ｄ又は７Ｄと同じものであり、外部認証データ１５Ａは、１回目の外部認証データ７Ａと同じものである。

【０１８７】次に、上記合成データが外部認証データ１５Ａと暗号データ１５Ｄとに分離され（Ｖ８）、外部認証データ１５Ａからは日付認証データ１５Ａ－Ｄが取出される（Ｖ９）。これにより１回目の外部認証機関９９による認証が確認される。

【０１８８】次に、暗号データ１５Ｄが作成者の公開鍵１６（＃１）を使用して復号化手段１７により復号化され、見出し付き特徴データ１８が生成される（Ｖ１０）。さらに、見出し１８Ｈと特徴データ１８Ｄとに分離される（Ｖ１１）。

【０１８９】一方、認証付き電子文書２８から、見出し付き暗号データ２７が取り除され、この元の電子文書１９から特徴抽出手段２０により特徴データ２１が抽出される（Ｖ１２）。そして、ステップＶ１１で分離された特徴データ１８Ｄと、特徴データ２１とが照合手段２２により照合され、同一性判定データ２２－Ｊが生成される（Ｖ１３）。

【０１９０】照合結果である同一性判定データ２２－Ｊにより、電子文書１９と電子文書１とが同一かどうかが判定され（Ｖ１４）、不一致と判断された場合には表示装置１１１から不一致が表示される（Ｖ１５）。一方、同一と判断された場合には、認証日付３１Ａ－Ｄ及び１５Ａ－Ｄとが表示され、さらに同一である旨の表示が行われる（Ｖ１６）。こうして、改竄防止を強化した電子文書の同一性判定が終了する。

【０１９１】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、外部認証機関９９において期間をおいて２度に渡って認証され暗号化された認証付き電子文書２８について、同一性を照合し外部認証を確認するようにしたので、改竄防止を強化した電子文書２８の同一性の判定を容易に行う事ができる。また、暗号解読の恐れが有る年数を経過する前に更に新しい暗号による文書の改竄防止ができるので、長期間の電子文書保管を行っても、裁判の場で文書の正当性が証明できるようになる。

【０１９２】本実施形態では、電子文書２８の如く１度の再認証（合計２回の外部認証）の電子文書２８の同一性判定を行う実施例を説明したが、電子文書２８を更に再認証した文書の同一性判定をしてもよい。認証の回数を重ねた場合は、復号の回数を重ねる事で電子文書の同一性判定が行える。

【０１９３】（第５の実施の形態）本実施形態では、第１又は第３の実施形態で説明した電子文書の改竄防止システムを利用した電子契約書作成システムについて説明する。

【０１９４】図１３は本発明の第５の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９及び図１１と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２及び図３に示す文書認証システム１０１及び外部認証システム１０２が用いられており、本実施形態の独自な機能部分は、文書認証プログラム１３３あるいは外部認証プログラム１３４に修正が加えられたことによるものである。

【０１９５】この電子文書の改竄防止システムは、契約者の一方である甲が使用する文書認証システム１０１（以下、甲システム１０１ａともいう）と、契約者の他方である乙が使用する文書認証システム１０１（以下、乙システム１０１ｂともいう）と、外部認証システム１０２とから構成されている。また、この電子文書の改竄防止システムは、甲乙間での契約を行うための電子契約書作成システムともなっている。なお、甲システム１０１ａと、乙システム１０１ｂと、外部認証システム１０２とは図１に示すようにネットワークで接続されている。

【０１９６】甲システム１０１ａは、秘密鍵４（＃１）として甲の秘密鍵４（甲）を用い、また見出し付き暗号データ６を外部認証システム１０２に代えて乙システム１０１ｂに送信する。さらに、甲システム１０１ａは、外部認証システム１０２から受け取る合成データ１１として見出し付き暗号データ４０を受け取り、電子文書１に付して電子契約書である認証付き電子文書４１を作成する他、第１又は第３の実施形態の文書認証システム１０１と同様に構成されている。

【０１９７】一方、乙システム１０１ｂは、甲システム１０１ａから受け取った見出し付き暗号データ６の中の暗号データ３２Ｄに乙の認証データ３２Ａを付加した結合データを生成し、見出し付き認証データ３２を作成する手段（図示せず）と、この結合データを乙の秘密鍵３３（乙）で暗号化する暗号化手段３４と、見出し付き認証データ３２の見出し３２Ｈ（３５Ｈ）と暗号化手段３４で暗号化された暗号データ３５Ｄとを結合して電子署名３５を作成する手段（図示せず）と、この電子署名３５を外部認証システムにネットワークを介して送信する手段（図示せず）とを備える他、第１又は第３の実施形態の文書認証システム１０１と同様に構成されている。

【０１９８】なお、甲システム１０１ａと乙システム１０１ｂは上記説明したそれぞれの各機能を組み合わせ、同一の処理が実行できるシステムとしてもよい。

【０１９９】また、外部認証システム１０２は、見出し付き認証データ７に代えて見出し付き認証データ３６について図４と同様な処理を施すように構成され、さらに見出し付き暗号データを乙システム１０１ｂでなく甲システム１０１ａに送信する他、第１又は第３の実施形態と同様に構成されている。すなわち、見出し付き認証データ３６は図４の見出し付き認証データ７、暗号データ３６Ｄは図４の暗号データ７Ｄ、外部認証データ３６Ａは図４の外部認証データ７Ａ、見出し３６Ｈは図４の見出し７Ｈに対応する。また、見出し付き暗号データ３９は図４の合成データ１０、見出し３９Ｈは図４の見出し

35

１０Ｈ、暗号データ３９Ｄは図４の暗号データ１０Ｄに対応する。さらに、暗号化手段３８は図４の暗号化手段９に対応し、秘密鍵３７は図４の秘密鍵８に対応する。なお、暗号データ３６Ｄは、甲と乙のそれぞれにより暗号化された甲乙の認証データであり、暗号データ３９はこの甲乙の認証データにさらに外部認証が与えられて暗号化されたものである。

【０２００】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図１３及び図１４を用いて説明する。

【０２０１】図１４は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０２０２】まず、甲システム１０１ａにおいて、外部記憶装置１１４、ハードディスク装置１２８から、あるいはネットワーク１００を介して電子文書１が読み込まれる（Ｗ１）。次に電子文書１から見出し部分が取出され、金額情報と印紙税支払者名が記入され、その他必要事項を編集して見出し３Ｈとする（Ｗ２）。

【０２０３】次に、電子文書１から特徴抽出手段２によって特徴データ３Ｄが抽出される（Ｗ３）。さらに特徴データ３Ｄが契約者甲の秘密鍵４（甲）を用いて暗号化手段５によって暗号化され暗号データ６Ｄが生成される（Ｗ４）。見出し３Ｈ（６Ｈ）と暗号データ６Ｄとが結合され契約者甲の電子署名データである見出し付き暗号データ６が生成される（Ｗ５）。

【０２０４】この契約者甲の電子署名データは甲システム１０１ａから契約者乙の使用する乙システム１０１ｂに電子文書１と共に送信される（Ｗ６）。なお、乙に電子文書１を送信するのは、乙が認証するに当たりその文書内容を確認できるようにするためである。

【０２０５】乙システム１０１ｂにおいては、まず、契約者甲の電子署名（見出し付き暗号データ６）と電子文書１が受信される（Ｗ７）。この受け取った電子署名データが見出し３２Ｈと暗号データ３２Ｄとに分離される（Ｗ８）。

【０２０６】次に、暗号データ３２Ｄに乙の認証データ３２Ａが結合されて結合データが生成される（Ｗ９）。この認証データ３２Ａには乙の名前と日付が含まれる。次に暗号データ３２Ｄと認証データ３２Ａが乙の秘密鍵３３を用いて暗号化手段３４によって暗号化され、暗号データ３５Ｄが生成される（Ｗ１０）。

【０２０７】そして、見出し３２Ｈ（３５Ｈ）と暗号データ３５Ｄとが結合されることで甲と乙の電子署名３５（見出し付き暗号データ３５）となる（Ｗ１１）。この電子署名３５は甲の秘密鍵４（甲）で暗号化された部分と乙の秘密鍵３３（乙）で暗号化された部分が含まれ、更に見出し６Ｈ及び認証データ３２Ａに甲乙の名前が含まれるため、実質的に両者の電子署名となるものである。また、見出し３５Ｈあるいは暗号データ３５Ｄに甲乙の正規の電子署名を含ませるようにしてもよい。

36

【０２０８】こうして生成された甲と乙の電子署名３５は外部認証機関９９の外部認証システム１０２にネットワーク１００を介して送信される（Ｗ１２）。

【０２０９】外部認証システム１０２においては、甲と乙の電子署名３５が受信される（Ｗ１３）。次に、甲と乙の電子署名３５が見出し３６Ｈと暗号データ３６Ｄとに分離される（Ｗ１４）。さらに暗号データ３６Ｄに外部認証機関の外部認証データ３６Ａが結合される（Ｗ１５）。外部認証データ３６Ａには外部認証機関９９の名前と日付および印紙税支払い済の記事が含まれる。印紙税の支払については、予め甲が外部認証機関９９との間で契約をしておく。

【０２１０】次に、暗号データ３６Ｄと認証データ３６Ａとが外部認証機関９９の秘密鍵３７を用いた暗号化手段３８によって暗号化され、暗号データ３９Ｄが生成される（Ｗ１６）。さらに、見出し３６Ｈ（３９Ｈ）と暗号データ３９Ｄが結合され甲乙及び外部認証機関９９の電子署名である見出し付き暗号データ３９が完成する（Ｗ１７）。この電子署名がネットワーク経由で甲システム１０１ａに送信される（Ｗ１８）。

【０２１１】甲システム１０１ａにおいては、電子署名である見出し付き暗号データ３９を見出し付き暗号データ４０として受け取る（Ｗ１９）。そして、この電子署名である見出し付き暗号データ４０が電子文書１と合成されて電子契約書４１（認証付き電子文書４１）が完成する。

【０２１２】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、甲と乙と外部認証機関９９とでそれぞれ電子文書１について認証を与え、かつそれぞれの秘密鍵で認証データを暗号化するようにしたので、作成された電子契約書に対する改竄を防止することができ、かつこれを証拠能力のある電子文書とすることができる。

【０２１３】つまり、電子契約書の改竄を行うとその電子文書１の有する特徴データが変化すること、最初に抽出された特徴データ３Ｄが契約者の甲乙および外部認証機関の全員で暗号化されている事によって電子契約書の改竄を行うと必ず発見できる事から、紙の代わりに電子文書での契約が可能になるものである。さらに、従来の紙の文書では改竄の有無を判定するには高度な技術が必要とされたが、本発明になる電屍文書の改竄防止システムでは容易に改竄の有無を証明できる。また、電子化により保管場所が削減されると共に遠隔地への電送が瞬時に行えるようになり、コンピュータによる検索が行えるようになる。

【０２１４】加えて紙の契約書では字句の誤りを訂正する為に捨て印を押す悪習が有ったが、電子化により、契約者間で瞬時に文書のやり取りが可能になるので、捨て印を押さなくても直ちに訂正して再署名が可能と成り、契約者間のトラブルの発生を防止できる。電子署名３５

に契約金額、印紙税支払者名が記載されているので、外部認証機関に電子文書そのものを送る必要が無く、秘密としたい事項が有る場合でも電子契約書を使用できる。

【０２１５】また、本実施形態では、電子文書１から特徴データを取り出して、これに甲乙、外部認証機関の認証を与えるようにしたが、本発明はこのような場合に限られるものでない。例えば元の電子文書１自体に文書作成者の関係者や上司が上司印等に相当するデータを付加し、当該上司印が付加された電子文書１から特徴データ３Ｄを取り出すようにすれば、実質的にその上司の認証をも付与された電子文書１を取り出すことが可能となる。元の電子文書を改竄すれば特徴データが変化するからである。

【０２１６】さらに、例えば本実施形態では、契約者が甲と乙の２人である場合を説明したが、本発明はこのような場合に限られるものではない。例えば契約者が甲、乙、丙の３者になる場合には、図１３での乙のステップが丙に付いても繰り返し行われるようにすれば３人が契約者の認証が入った上記と同様な電子契約書を作成することができる。また、契約者に更に丁がいる場合には丁に付いてもこの乙のステップを繰り返し行えばよい。従って、契約者の人数には、かかわらず電子契約書を作成し使用できることとなる。

【０２１７】（第６の実施の形態）本実施形態では第５の実施形態で作成した電子契約書が真正なものであることを確認し、また契約者や外部認証機関の付した各認証日付等の認証情報を取り出すシステムについて説明する。

【０２１８】図１５は本発明の第６の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９、図１１及び図１３と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図６に示す認証文書認証システム１０３が用いられており、本実施形態の独自な機能部分は、認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０２１９】この電子文書の改竄防止システムは、図１に示した認証文書確認システム１０３として構成されるものであり、電子契約書の照合システムでもある。

【０２２０】認証文書確認システム１０３は、電子契約書４１（認証付き電子文書４１）に付された見出し付き暗号データ４０に対し、外部認証機関９９の公開鍵４２（認）、契約者乙の公開鍵４５（乙）及び契約者甲の公開鍵４８（甲）による復号を行い、外部認証機関の認証事実及び認証日付、乙の認証事実及び認証日付を取り出して認証確認を行うとともに、特徴データ５０を取出し、一方、見出し付き暗号データ４０を取り除いた電子文書１から特徴データ５２を取出し、両特徴データ５０，５２を照合して同一性判定を行うようになっている。

【０２２１】このために電子文書の改竄防止システムには、電子契約書４１から見出し付き暗号化データ４０を取り出す手段（図示せず）と、これに含まれる暗号データ４０Ｄを外部認証機関の公開鍵４２（認）で復号する復号化手段４３と、復号化手段４３により復号化された外部認証データ４４Ａから外部認証機関の認証事実と認証日付を日付認証４４Ａ－Ｄとして取り出す手段（図示せず）と、復号化手段４３により復号化された暗号データ４４Ｄを乙の公開鍵４５（乙）で復号化する復号化手段４６とが設けられている。さらに、復号化手段４６により復号化された乙の認証データ４７Ａから乙の認証事実と認証日付を日付認証４７Ａ－Ｄとして取り出す手段（図示せず）と、復号化手段４６により復号化された暗号データ４７Ｄを甲の公開鍵４８（甲）で復号化する復号化手段４９とが設けられている。一方、電子契約書４１から見出し付き暗号化データ４０が除かれた元の電子文書１から特徴抽出を行って特徴データ５２を生成する特徴抽出手段５１と、この特徴データ５２と復号化手段４９により復号化された特徴データ５０Ｄとを照合して電子文書の同一性判定５３－Ｊを行う照合手段５３とが設けられている。

【０２２２】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図１５を用いて説明する。

【０２２３】まず、外部記憶装置１１４、ハードディスク装置１２８から、あるいはネットワーク１００を介して電子契約書４１が読み込まれ、認証データである見出し付き暗号データ４０が取出される。この見出し付き暗号データ４０から暗号データ４０Ｄが取出され、外部認証機関の公開鍵４２を用いて復号化手段４３により復号化され暗号データ４４Ｄと認証データ４４Ａが生成される。暗号データ４４Ｄは図１３の暗号データ３６Ｄに対応するもので、外部認証データ４４Ａは図１３の外部認証データ３６Ａに対応するものである。

【０２２４】外部認証データ４４Ａからは日付認証４４Ａ－Ｄが取出される。暗号データ４４Ｄは契約者乙の公開鍵４５を用いて復号化手段４６によって復号化され、暗号データ４７Ｄと認証データ４７Ａとが取出される。暗号データ４７Ｄは図１３の暗号データ３２Ｄに対応し、認証データ４７Ａは図１３の乙の認証データ３２Ａに対応する。

【０２２５】認証データ４７Ａからは乙の日付認証４７Ａ－Ｄが取出される。暗号データ４７Ｄは契約者甲の公開鍵４８を用いて復号化手段４９によって復号化され特徴データ５０Ｄが取出される。

【０２２６】一方電子文書４１から認証データ４０を取り除いたデータは電子文書１のデータに相当する。電子文書１に相当するデータから特徴抽出手段５１によって特徴を抽出して特徴データ５２が得られる。

【０２２７】照合手段５３で特徴データ５０Ｄと特徴デ

ータ５２とが比較照合され、同一性判定５３－Ｊが得られる。同一性判定５３－Ｊが同一を示していれば電子文書の改竄は行われていないが、そうでない時には改竄が行われている。

【０２２８】また、甲作成の電子文書１に対する外部認証機関及び乙の認証事実と、認証日付が表示されることになり、契約書についての正当性が確認される。

【０２２９】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴データ５０Ｄ，５２による同一性判定及び甲作成の電子文書１に対する外部認証機関及び乙の認証事実並びに認証日付が確認されるので、電子契約書の同一性の判定を効果的に行う事ができ、裁判の場で文書の正当性が証明できるようになる。

【０２３０】なお、本実施形態では、契約者が甲と乙の２者の場合を説明したが、本発明はこの場合に限られるものではない。契約者が、甲、乙、丙の３者になる場合には図１５での乙のステップが丙に付いても繰り返し行われるだけでよい。さらに契約者に更に丁がいる場合は丁に付いても乙のステップを繰り返し行えばよい。従って、契約者の人数にはかかわらない、複数人の間でかわされた電子契約書を確認することができる。

【０２３１】（第７の実施の形態）本実施形態は、上記各実施形態における例えば図４や図７の見出し１１Ｈの編集手段の具体的な例を説明するとともに、認証付き電子文書１２を表示あるいは印刷させるときの表示編集手段について説明する。

【０２３２】図１６は本発明の第７の実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９、図１１、図１３及び図１５と同一部分には同一符号を付し、その説明を省略する。本実施形態のシステムには、図２に示す文書認証システム１０１、あるいは図６に示す認証文書確認システム１０３が用いられている。本実施形態の独自な機能部分は、文書認証プログラム１３３あるいは認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０２３３】この電子文書の改竄防止システムは、図１に示す文書認証システム１０１、あるいは認証文書確認システム１０３に以下に説明する手段が付加されてなる。なお、以下、文書認証システム１０１の場合を例にとって説明する。

【０２３４】本実施形態の文書認証システム１０１では、第１、第３、第５実施形態と同様な構成の他、表示印刷手段を備え、また、見出しの編集手段が具体的に示される。

【０２３５】見出しの編集手段には、見出し１１Ｈを編集する際に、印鑑等が押された表示物をイメージ情報である印影５４として取り込むスキャナ１１５（図２等）と、この印影５４を電子印鑑６０の一部に加える手段（図示せず）と、印影５４から特徴抽出して特徴データを生成する特徴抽出手段５５と、特徴データ５６を秘密鍵４で暗号化する暗号化手段５８と、暗号化された暗号化印影５９を電子印鑑６０の一部に加える手段（図示せず）と、電子印鑑６０に名前等を加える入力手段（入力装置１１２）と、完成した電子印鑑６０を見出し１１Ｈ（３Ｈ）として見出し付き特徴データ３（図１６では合成データ１１）に加える手段（図示せず）とが設けられている。なお、電子印鑑６０は、印影５４と暗号化印影５９と所有者の名前を合成してなるものである。

【０２３６】一方、表示印刷手段には、合成データ１１の見出し１１Ｈから日付・署名・印影情報６１を取り出す手段（図示せず）と、これらのデータを表示領域内に収まるように整形する手段６２と、一方、認証付き電子文書１２から電子文書１をと取り出す手段（図示せず）と、取り出された電子文書１の中に記載されるタグ及び表示領域情報１Ｔに整形された日付・署名・印影情報を重ね合わせる手段（図示せず）と、この重ね合わされた表示文書６３を印刷あるいは表示する手段（表示装置１１１、印刷装置１１３）とが設けられている。

【０２３７】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図１６、図１７、図１８及び図１９を用いて説明する。

【０２３８】まず電子印鑑６０を生成する処理を図１６および図１７により説明する。

【０２３９】図１７は本実施形態の電子文書の改竄防止システムの電子印鑑生成処理を示す流れ図である。

【０２４０】まず、電子印鑑の所有者名が入力装置１１２により入力される（Ｘ１）。次に印影データ５４が読込まれる（Ｘ２）。印影データは紙に印鑑を押したものをスキャナ１１５で読み取り電子化したものが用いられる。

【０２４１】次に、印影データ５４から特徴抽出手段５５で特徴が抽出され特徴データ５６が生成される（Ｘ３）。特徴データ５６が所有者の秘密鍵４を使用した暗号化手段５８により暗号化され暗号化印影５９が生成される（Ｘ４）。印影データ５４、暗号化印影５９及びステップＸ１で入力した所有者名が一つのデータとして纏められ電子印鑑６０が生成される（Ｘ５）。そして、電子印鑑６０が第１の実施の形態の図１の見出しデータ３Ｈに入れられる。この結果図１６の認証付き電子文書１２の見出し１１Ｈに電子印鑑６０のデータが保存されることとなる（Ｘ６）。

【０２４２】次に改竄を防止した電子印鑑の照合処理を図１８により説明する。

【０２４３】図１８は本実施形態の電子文書の改竄防止システムの電子印鑑照合処理を示す流れ図である。

【０２４４】この照合処理は、電子文書１自体の同一性判定と別途に行われるものであり、見出し１１Ｈに含ま

れる電子印鑑（電子署名）の正当性を評価するものである。なお、この処理の手段は特に図１６では示していないが、その手段は文書認証プログラム１３３あるいは認証文書確認プログラム１３５とシステムのハードウエアで実現されるものであり、図１８で示される処理を実現するものである。

【０２４５】まず、所有者名が入力される（Ｙ１）。所有者名に従いその所有者の公開鍵が外部記憶装置１１４、ハードディスク装置１２８から、あるいはネットワーク１００を介して読込まれる（Ｙ２）。次に、電子印鑑６０の中にある暗号化印影が公開鍵を用いて復号化される（Ｙ３）。

【０２４６】一方、電子印鑑６０の中にある印影データから特徴抽出が行われる（Ｙ４）。次に、ステップＹ３で復号化した特徴データとステップＹ４で抽出した特徴データとの照合が行われる（Ｙ５）。

【０２４７】この照合結果の判定が行われ（Ｙ６）、印鑑が不一致であれば表示装置１１１にその旨表示される。一方、印鑑が一致していればその旨が表示される。

【０２４８】次に電子文書に電子印鑑や日付を重ね合わせて表示または印刷できるように、文書及び見出しを編集する処理を図１６および図１９により説明する。

【０２４９】図１９は本実施形態の電子文書の改竄防止システムの文書見出し編集処理を示す流れ図である。

【０２５０】まず、電子文書１の編集が行われる（Ｚ１）。この処理は電子文書１そのものの作成作業でありシステム使用者による作業である。さらに電子文書１にシステム使用者による作業で表示領域が設定される（Ｚ２）。この段階で日付・署名・印影情報を表示する場所が決められる。

【０２５１】次に電子文書１の内部にステップＺ２作成した表示領域にタグおよび表示領域情報１Ｔを埋め込む（Ｚ３）。

【０２５２】ここから見出し編集に入り、日付・署名・印影情報６１が編集される（Ｚ４）。さらに見出しデータ１１Ｈに埋め込むタイトル情報が入力されるか、もしくは電子文書内のタイトル部分が指定されその値が見出し１１Ｈに取り込まれる（Ｚ５）。そして見出し１１Ｈが保存される（Ｚ６）。

【０２５３】次に、電子文書１が保存される（Ｚ７）。なお、電子文書１には見出し１１Ｈ自体が埋め込まれる訳ではないので、ステップＺ３の電子文書１へのタグおよび表示領域情報１Ｔ埋め込みの後に直ちにステップＸ７の文書保存を行ってもよい。

【０２５４】以上の処理により、電子文書１のどの場合に日付・署名・印影情報６１を表示したらよいかが記録されるので、電子文書１を表示または印刷する時には、図１６で示したように、電子文書上に日付・署名・印影を重ね合わせて表示文書６３とすることができる。

【０２５５】これにより、改竄を防止した電子文書１２に改竄を防止した電子印鑑６０が付けられ、さらにこれらを重ね合わせた表示文書６３として、表示または印刷されることになる。

【０２５６】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴抽出を行って暗号化した電子印鑑６０を見出し３Ｈに加えるようにしたので、電子印鑑６０の印影改竄の有無が判定でき、電子文書に改竄を防止した印影を張り付けることができる。

【０２５７】また、このように改竄を防止した印影を、改竄を防止しまた改竄の有無判定ができる電子文書と合わせて、表示や印刷ができるようにしたので、この改竄防止が保障された表示や印刷によって、従来の紙の文書と同様な運用が可能となる。従来の紙の文書と同じ運用が可能でありながら、伝送で文書を瞬時に遠隔地に送る事ができる為その効果は非常に大である。なお、この場合、表示文書６３に表示される電子文書は、同一性判定及び認証確認を行ったものを用いればより効果的である。

【０２５８】なお、本実施形態では、１つの電子印鑑６０を見出し３Ｈに入れる場合で説明したが、本発明はこれに限られるものではない。見出しデータは編集する事が可能である為、図４や図７における使用の外に、図１３や図１５の使用においても運用する事ができ、電子文書の中に甲の日付・署名・印影と乙の日付・署名・印影を入れる事ができる。この場合にも電子文書１そのものは改竄される事が無い事は言うまでもない。

【０２５９】さらに、以上の説明では紙に印鑑を押したものをスキャナ１１５で読取り電子化した印影を用いるとしたが、紙に手書きのサインをしてスキャナ１１５で読取り電子化した電子サインを用いてもよい。

【０２６０】（第８の実施の形態）本実施形態は、上記第１～第７の実施形態で使用される特徴抽出手段の構成動作の例を説明する。

【０２６１】図２０は本発明の第８の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図である。

【０２６２】また、図２１は本実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９、図１１、図１３、図１５及び図１６と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２に示す文書認証システム１０１、あるいは図６に示す認証文書認証システム１０３が用いられている。本実施形態の独自な機能部分は、文書認証プログラム１３３あるいは認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０２６３】この電子文書の改竄防止システムは、図１に示す文書認証システム１０１、あるいは認証文書確認システム１０３における特徴抽出手段として以下に説明

する手段が設けられて構成される。なお、以下、文書認証システム１０１の場合を例にとって説明する。

【０２６４】図２１に示すように、文書認証システム１０１又は認証文書確認システム１０３の特徴抽出手段２（２０，５１，５５）は、電子文書１から特徴データ３Ｄを生成する。

【０２６５】この特徴抽出手段２には、データＳ＿ｓｕｍを格納する部分とデータＩＳ＿ｓｕｍを格納する２５６個の配列と、図示しない処理手段とが設けられている。この処理手段は以下に説明する処理を実現する機能実現手段である。

【０２６６】まず、図２０は特徴抽出手段のデータの流れを示している。

【０２６７】同図において、電子文書やファイル等のデータそのもの，すなわちＳｔｒｅａｍは、電子文書データ並びＳをなしている。この電子文書データ並びＳは、２５６バイトずつに区切られた電子文書データ並び部分Ｓ１、Ｓ２、Ｓ３、．．．、Ｓｎにより構成される。

【０２６８】このＳｔｒｅａｍから生成されるＳ＿ｓｕｍ＿ｓｔｒｅａｍは、合計データ並びＳ＿ｓ＿ｓｔｒｅａｍをなしている。この合計データ並びＳ＿ｓ＿ｓｔｒｅａｍは、合計データ並び部分ＳＳ１、ＳＳ２、ＳＳ３、．．から構成される。ＳＳ１は、Ｓ１、Ｓ２、Ｓ３、．．、Ｓ２５６それぞれの合計値を２５６個のデータの並びとしたものである。同様に、ＳＳ２は、Ｓ２５７～Ｓ５１２それぞれの合計値をデータの並びとしている。

【０２６９】一方、ＳｔｒｅａｍからはＩｎｔｅｒｖａｌｅｄ　Ｓｔｒｉｎｇとして間隔を置いたデータ並びＩＳが生成される。この間隔を置いたデータ並びＩＳは間隔を置いたデータ並び部分ＩＳ１、ＩＳ２、ＩＳ３、．．、ＩＳｎから構成される。ここで、ＩＳ１は、Ｓ１、Ｓ２、Ｓ３、．．、Ｓ２５６の各先頭データを順次２５６個並べたものであり、ＩＳ２は、Ｓ１、Ｓ２、Ｓ３、．．、Ｓ２５６の各２番目のデータを順次２５６個並べたものである。以下同様に、ＩＳ３～ＩＳ２５６が構成される。ＩＳ２５７は、Ｓ２５７～Ｓ５１２の各先頭データを順次２５６個並べたものである。以下同様である。

【０２７０】このＩｎｔｅｒｖａｌｅｄ　Ｓｔｒｉｎｇから生成されるＩＳ＿ｓｕｍ＿ｓｔｒｅａｍは、間隔を置いた合計データ並びＩＳ＿ｓ＿ｓｔｒｅａｍをなしている。この間隔を置いた合計データ並びＩＳ＿ｓ＿ｓｔｒｅａｍは、間隔を置いた合計データ並び部分ＩＳＳ１、ＩＳＳ２、ＩＳＳ３、．．から構成される。この間隔を置いた合計データ並び部分ＩＳＳ１、ＩＳＳ２、ＩＳＳ３、．．は、間隔を置いたデータ並び部分ＩＳ１～ＩＳｎから生成され、その生成方法は、Ｓ１～ＳｎからＳＳ１、ＳＳ２、ＳＳ３、．．を生成する方法と同じである。

【０２７１】なお、最終的には、合計データ並びＳ＿ｓ＿ｓｔｒｅａｍと間隔を置いた合計データ並びＩＳ＿ｓ＿ｓｔｒｅａｍとが特徴データ３Ｄとなる。

【０２７２】ここで、図２０と図２１との関係を説明すると以下の通りである。

【０２７３】Ｓ１は２５６バイトのデータの並びで、このＳ１のデータの合計値が図２１のＳ＿ｓｕｍに格納され、Ｓ＿ｓｕｍの値がＳ＿ｓ＿ｓｔｒｅｍに出力される。Ｓ＿ｓ＿ｓｔｒｅｍはワード（１６ビット）のデータの並びで２５６バイトの合計値を取っても桁落ちは発生しない。同様にＳ１に続くデータの並びＳ２に対しても合計値がＳ＿ｓ＿ｓｔｅｒａｍに出力される。以下、Ｓ３からＳｎに至るまで同様に行われる。

【０２７４】ＩＳ１は２５６バイトのデータの並びでＳ１の先頭１バイト、Ｓ２の先頭１バイトＳ３のい先頭１バイトと続き、Ｓ２５６の先頭１バイトまでが格納される。ＩＳ２は同様に２５６バイトのデータの並びでＳ１の２バイト目、Ｓ２の２バイト目、Ｓ３の２バイト目と続き、Ｓ２５６の２バイト目までが格納される。同様にＩＳ３は同様に２５６バイトのデータの並びでＳ１の３バイト目、Ｓ２の３バイト目、Ｓ３の３バイト目と続き、Ｓ２５６の３バイト目までが格納される。ＩＳ２５６はＳ１の２５６バイト目、Ｓ２の２５６バイト目、Ｓ３の２５６バイト目と続き、Ｓ２５６の２５６バイト目までが格納される。ＩＳ１からＩＳ２５６までのデータはそれぞれ合計が取られて、図２１のＩＳ＿ｓｕｍ［０］からＩＳ＿ｓｕｍ［２５５］に格納され、ＩＳ＿ｓｕｍの並びがＩＳ＿ｓ＿ｓｔｒｅａｍに出力される。ＩＳ＿ｓ＿ｓｔｒｅａｍはワードのデータの並びで２５６バイトの合計値を取っても桁落ちは発生しない。

【０２７５】こうしてＳ＿ｓ＿ｓｔｒｅａｍとＩＳ＿ｓ＿ｓｔｒｅａｍからなる特徴データが得られるが、次にこの処理のフローを図２２で説明する。

【０２７６】図２２は本実施形態の電子文書の改竄防止システムの特徴データ抽出の処理の一例を示す流れ図である。

【０２７７】まず、全てのデータが初期化される（Ａ１）。次に電子文書データ並びＳのデータが有るかどうかが調べられる（Ａ２）。

【０２７８】データが有る場合にはステップＡ３に移り、Ｓから１バイトが読込まれる。一方、データが無い場合にはステップＡ４に移り終了処理が行われる。

【０２７９】ステップＡ３でＳから１バイトを読んだ後は、読んだ値がＳ＿ｓｕｍとＩＳ＿ｓｕｍ［ｉ］に加算される（Ａ５）。

【０２８０】次に、ｉが２５５かどうかが調べられる（Ａ６）。ｉが２５５でない場合にはｉを１増加させ（Ａ７）、ステップＡ２に戻る。一方、ｉが２５５の場合には（Ａ６）、Ｓ＿ｓｕｍの値がＳ＿ｓ＿ｓｔｒｅａｍに出力されｉがゼロに戻される（Ａ８）。

【０２８１】次に、ｊが２５５かどうかが調べられる（Ａ９）。ｊが２５５でない場合にはｊを１増加させ（Ａ１０）、ステップＡ２に戻る。一方、ｊが２５５の場合には（Ａ９）、ＩＳ＿ｓｕｍ［1］からＩＳ＿ｓｕｍ［２５５］までの値をＩＳ＿ｓ＿ｓｔｒｅａｍに出力してｊをゼロに戻し（Ａ１１）、ステップ２に戻る。

【０２８２】このような処理により、電子文書のデータが１バイトづつ順次読込まれ、全データが処理されるまで図２０のデータ（Ｓ＿ｓ＿ｓｔｒｅａｍ，ＩＳ＿ｓ＿ｓｔｒｅａｍ）が生成されつづけ、特徴データ３Ｄとして出力される。

【０２８３】このＳ＿ｓ＿ｓｔｒｅａｍ及びＩＳ＿ｓ＿ｓｔｒｅａｍを特徴データとした場合、電子文書データ並びＳ（電子文書１や印影５４等）のどの１バイトの値が変化してもＳ＿ｓ＿ｓｔｒｅａｍの何処かの１ワードが変化する。また、電子文書データ並びＳのどの２バイトを入れ替えてもＩＳ＿ｓ＿ｓｔｒｅａｍの何処かの１ワードが変化する。

【０２８４】例えば、Ｓ１のデータ部分内部でデータの入れ替えを行うと、Ｓ１の合計値は変化しないがＩＳ＿ｓｕｍ［0］からＩＳ＿ｓｕｍ［２５５］の何処かの値は必ず変化する。これによって電子文書１のどのデータを改竄しても改竄の事実が発見される。また、Ｓ１の２５６バイトのデータが１ワードに圧縮され、ＩＳ１の２５６バイトのデータが１ワードに圧縮される事から、元のデータの１／６４のサイズにデータが圧縮される。また、このように生成される特徴データは、データの圧縮が一方向性であり、特徴データから元のデータを再現する事はできない。

【０２８５】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴抽出手段により、図２０に示すようなＳ＿ｓ＿ｓｔｒｅａｍ及びＩＳ＿ｓ＿ｓｔｒｅａｍを特徴データとして生成するようにしたので、元のデータのどの部分がどの様に変化してもその変化を発見することができる。また、特徴データは元のデータに比較してデータサイズが大幅に小さくなり取り扱いが容易である。また、特徴データの取出し方がシンプルで演算を高速にすることができる。

【０２８６】さらに、特徴データから元のデータを再現できない事から、外部認証機関９９に電子文書１を開示したくない場合には、認証対象を不開示のまま電子文書の認証を行うことができる。特徴データを用いる方法では電子文書の認証にその文書自体の引き渡しが必要ないからである。

【０２８７】（第９の実施の形態）本実施形態は、上記第１～第７の実施形態で使用される特徴抽出手段の構成動作の他の例を説明する。

【０２８８】図２３は本発明の第９の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図であり、図２０と同一部分には同一符号を付してその説明を省略する。

【０２８９】また、本実施形態の電子文書の改竄防止システムには、図２に示す文書認証システム１０１、あるいは図６に示す認証文書認証システム１０３が用いられ、特徴抽出手段として以下に説明する手段が設けられている。なお、本実施形態の独自な機能部分は、文書認証プログラム１３３あるいは認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０２９０】本実施形態における特徴抽出は、Ｓ＿ｓ＿ｓｔｒｅａｍ及びＩＳ＿ｓ＿ｓｔｒｅａｍが抽出されるまでは第８の実施形態と同様に行われる。また、Ｓ＿ｓ＿ｓｔｒｅａｍからＳ＿ｓ＿ｓｔｒｅａｍ′、ＩＳ＿ｓ＿ｓｔｒｅａｍからＩＳ＿ｓ＿ｓｔｒｅａｍ′が生成され、これらのＳ＿ｓ＿ｓｔｒｅａｍ′及びＩＳ＿ｓ＿ｓｔｒｅａｍ′が最終的な特徴データ３Ｄとして使用される。なお、Ｓ＿ｓ＿ｓｔｒｅａｍ′及びＩＳ＿ｓ＿ｓｔｒｅａｍ′はロングワード（３２ビット）で構成される。

【０２９１】具体的な処理としては以下のようになる。

【０２９２】まず、ＳＳ１等とＩＳＳ１等を生成する手前までは第８の実施形態と同様である。第８の実施の形態では実際の処理においてはＳＳ１等とＩＳＳ１等を２５６ワード単位で区切らずにＳ＿ｓ＿ｓｔｒｅａｍ及びＩＳ＿ｓ＿ｓｔｒｅａｍとしてそのまま出力していた。これに対して図２３においてはＳ１、Ｓ２、Ｓ３、．．、Ｓｎを２５６バイトずつ合計して成る値の列を２５６ワードづつＳＳ１、ＳＳ２…ＳＳ２５６の合計値のロングワードの列にしてＳ＿ｓ＿ｓｔｒｅａｍ′に出力する。また、ＩＳ１、ＩＳ２、ＩＳ３、．．、ＩＳ２５６の合計値のロングワードの列をＩＳ＿ｓ＿ｓｔｒｅａｍ′に出力する。

【０２９３】いいかえると、Ｓ＿ｓ＿ｓｔｒｅａｍ′には、ＳＳ１、ＳＳ２、．．それぞれの合計値が順次データ並びとして出力され、同様に、ＩＳ＿ｓ＿ｓｔｒｅａｍ′には、ＩＳＳ１、ＩＳＳ２、．．それぞれの合計値が順次データ並びとして出力される。

【０２９４】これによって、図２０ではＳ＿ｓ＿ｓｔｒｅａｍはワードのストリームであったが、図２３ではＳ＿ｓ＿ｓｔｒｅａｍ′はロングワードのストリームとなる。同様に、図２０ではＩＳ＿ｓ＿ｓｔｒｅａｍはワードのストリームであったが、図２３ではＩＳ＿ｓ＿ｓｔｒｅａｍはロングワードのストリームとなる。これによりデータ量は更に１／１２８に圧縮され、最初の１／８１９２の大きさになる。

【０２９５】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴抽出手段により、図２３に示すようなＳ＿ｓ＿ｓｔｒｅａｍ′及びＩＳ＿ｓ＿ｓｔｒｅａｍ′を特徴データとして生成するようにしたので、第８の実施形態と同様な効果が得られる他、第８の実施形態の場合よりも更に特徴データ

をコンパクトなものとすることができる。

【０２９６】なお、第９の実施形態では第８の実施形態に対してデータの２５６個毎の合計を１回余分に行っているが、１回だけでは無く更に繰り返してデータを圧縮してもよい。このようにすればより一層特徴データをコンパクトなものとすることができる。

【０２９７】（第１０の実施の形態）本実施形態は、上記第１～第７の実施形態で使用される特徴抽出手段の構成動作のさらに他の例を説明する。

【０２９８】図２４は本発明の第１０の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図である。

【０２９９】また、図２５は本実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９、図１１、図１３、図１５及び図１６と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２に示す文書認証システム１０１、あるいは図６に示す認証文書認証システム１０３が用いられている。本実施形態の独自な機能部分は、文書認証プログラム１３３あるいは認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０３００】この電子文書の改竄防止システムは、図１に示す文書認証システム１０１、あるいは認証文書確認システム１０３における特徴抽出手段として以下に説明する手段が設けられて構成される。なお、以下、文書認証システム１０１の場合を例にとって説明する。

【０３０１】図２５に示すように、文書認証システム１０１又は認証文書確認システム１０３の特徴抽出手段２（２０，５１，５５）は、電子文書１から特徴データ３Ｄを生成する。

【０３０２】特徴抽出手段２には、セパレータテーブル２Ｔ及び単語配列２Ｗが設けられている。

【０３０３】一方、図２４において、電子文書１は単語とセパレータの並びで構成される。セパレータというのは、文書中において空白や句読点等の単語を分離するものである。単語配列２Ｗは単語のデータの並びとその順番で構成される。一方、特徴データ３Ｄは単語配列２Ｗのデータ並びの順番データの並びで構成される。

【０３０４】また、セパレータテーブル２Ｔは、予めセパレータとして使用するものを登録したものである。一方、単語配列２Ｗは、単語を格納する領域と配列の順番からなっている。

【０３０５】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムにおける特徴抽出処理について説明する。

【０３０６】まず、図２４で示すように、単語とセパレータから構成された電子文書１の先頭から順次データが読み込まれ、セパレータとセパレータで区切られたデータが単語とみなされる。見つけた単語のうち新しいものが単語配列２Ｗに登録され、その単語の配列番号が特徴データ３Ｄに書き出される。すなわちこの配列番号の並びそのものが特徴データとなる。

【０３０７】つまり、特徴抽出手段２により読み込まれた１文字がセパレータテーブル２Ｔのデータと比較され、セパレータでなければ次の１文字が読込まれる。順次読込みが行われ、読み込みを続けて得られた文字列が単語として検出される。この場合に、当該文字列が新しい単語であるか否かが判定される。そして新しい単語の場合には文字配列２Ｗに登録し登録番号を特徴データ３Ｄとして書き出す。既に出てきた単語の場合にはその登録番号を特徴データ３Ｄに書き出す。

【０３０８】この処理を図２６を用いてより具体的に説明する。

【０３０９】図２６は本実施形態の電子文書の改竄防止システムの特徴データ抽出の処理の一例を示す流れ図である。

【０３１０】まず、全てのデータが初期化される（Ｂ１）。次に、電子文書１のデータがあるかどうか調べられ（Ｂ２）、データがある場合には１文字分が読込まれる（Ｂ３）。データが無い場合には（Ｂ２）終了処理が行われる（Ｂ４）。

【０３１１】次に、読込んだ１文字がセパレータかどうかがセパレータテーブル２Ｔのデータとの比較により行われる（Ｂ５）。読込んだ１文字がセパレータの場合には（Ｂ５）、セパレータテーブル２Ｔとセパレータの比較が行われる（Ｂ６）。一方、読込んだ１文字がセパレータでない場合には（Ｂ５）、その文字をバッファに入れてステップＢ２に戻る（Ｂ７）。

【０３１２】ステップＢ６の後、配列２Ｗのテーブルデータ（ハッシュテーブル）とバッファデータの比較が行われる（Ｂ８）。なお、ステップＢ６はセパレータ自体の種類を決定するものであり、ステップＢ８はバッファの中に構成された単語の種類を決定するものである。

【０３１３】次に、ステップＢ６の結果よりテーブルデータ（配列２Ｗ）とセパレータが同じでない場合には（Ｂ９）、データがテーブル２Ｗに登録され（Ｂ１０）ステップＢ１１に移る。一方、同じ場合には（Ｂ９）、ステップＢ１０を行わずにステップＢ１１に移る。

【０３１４】ステップＢ１１では、テーブルデータ（配列２Ｗ）とバッファデータが同じでない場合には、バッファデータがハッシュテーブル２Ｗに登録され（Ｂ１２）、ステップＢ１３に移動する。一方、同じ場合には（Ｂ１１）ステップＢ１２を行わずにステップＢ１３に移動する。

【０３１５】そして、ステップＢ１３では、特徴データ３Ｄにステップ９～Ｂ１２で決定されたセパレータと単語それぞれのテーブル番号が出力される。その後ステップＢ２に戻る。

【０３１６】以上により電子文書１の特徴がハッシュテ

ーブルのテーブル番号並びとして抽出され特徴データ３Ｄとして得られる。

【０３１７】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴抽出手段により単語とセパレータのテーブル番号の並びを特徴データとして抽出するようにしたので、元のデータのどの部分がどの様に変化してもその変化を発見することができる。また、元のデータに比較してデータのサイズが大幅に小さくなり取り扱いが容易である。さらに特徴データから元のデータを再現できない事から、外部認証機関に電子文書を開示したくない場合であっても電子文書の認証を行うことができる。

【０３１８】（第１１の実施の形態）本実施形態は、第１～第７の実施形態で説明した電子文書の改竄防止システムにおける各文書認証システム１０１、外部認証システム１０２及び認証文書確認システム１０３を使用するにあたり、そのシステム使用者を確認するための情報を生成し、また、各システムで用いられる暗号鍵（秘密鍵、公開鍵等）を生成する手段について説明する。

【０３１９】図２７は本発明の第１１の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９、図１１、図１３、図１５及び図１６と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２に示す文書認証システム１０１、図３に示す外部認証システム１０２あるいは図６に示す認証文書認証システム１０３が用いられている。本実施形態の独自な機能部分は、文書認証プログラム１３３、外部認証プログラム１３４あるいは認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０３２０】この電子文書の改竄防止システムは、図１に示す文書認証システム１０１、外部認証システム１０２あるいは認証文書確認システム１０３と同様な構成に、以下に各手段が付加されて構成される。なお、以下、文書認証システム１０１の場合を例にとって説明する。

【０３２１】図２７に示す文書認証システム１０１は、システム使用者の指紋を読み取って特徴抽出を行い、この特徴データ６７、別途入力されたパスワード６８及び乱数を用いて暗号鍵７１，７４，７５，７７Ｓ，７７Ｋを生成するとともに、さらに使用者氏名、ＩＤ（識別情報）、パスワード、指紋及び生成した暗号鍵等から本人認証データ７８を生成するものである。この本人認証データ７８は、後述する第１２の実施形態においてシステム使用者を確認するのに用いられる。

【０３２２】この本人認証データ７８を生成するために文書認証システム１０１には、指紋読取り機６４と、イメージデータとして読み取られた指紋６５から特徴データ６７を抽出する特徴抽出手段６６と、入力装置１１２から入力されたパスワード６８及び氏名・ＩＤ６９のうちパスワード６８と特徴データ６７から暗号鍵７１を生成する暗号鍵生成手段７０と、乱数発生器７２と、乱数発生器７２から発生した乱数、パスワード６８及び特徴データ６７から秘密鍵７４及び公開鍵を生成する秘密鍵公開鍵生成手段７３と、暗号鍵７１及び秘密鍵７４から暗号化秘密鍵７７Ｓ及び暗号化暗号鍵７７Ｋを生成する暗号化手段とが設けられている。さらに、文書認証システム１０１には、指紋６５、暗号化秘密鍵７７Ｓ、暗号化暗号鍵７７Ｋ、パスワード６８及び氏名・ＩＤ６９を取り込み、指紋７８Ｆ、暗号化秘密鍵７８Ｓ、暗号化暗号鍵７８Ｋ、パスワード７８Ｐ及び氏名・ＩＤ７８Ｎからなる本人認証データ７８を作成する手段（図示せず）とが設けられている。

【０３２３】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図２７及び図２８を用いて説明する。

【０３２４】図２８は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０３２５】本動作は文書認証システム１０１のシステム起動時等における本人認証用データを作成する手続きである。

【０３２６】このためにまず、入力装置１１２により、最初に氏名・ＩＤデータ６９とパスワード６８が入力されてシステムが起動される（Ｃ１）。次に、指紋読取り機６４が起動され指紋が読取られる（Ｃ２）。これにより、指紋データ６５が得られる。

【０３２７】次に、指紋データ６５から特徴抽出手段６６によって特徴データ６７が抽出される（Ｃ３）。さらにパスワード６８と特徴データ６７とが使用され暗号鍵生成手段７０により暗号鍵７１が生成される（Ｃ４）。

【０３２８】次に、パスワード６８、乱数発生器７２および特徴データ６７が使用され秘密鍵公開鍵生成手段７３により秘密鍵７４と公開鍵７５が生成される（Ｃ４）。本実施形態では秘密鍵公開鍵生成手段７３としてＲＳＡ方式に対応したものを用いている。なお、ＤＥＳ等を用いてもよい。

【０３２９】次に、暗号鍵７１と秘密鍵７４とが暗号化手段７６により暗号化され暗号化秘密鍵７７Ｓと暗号化暗号鍵７７Ｋが生成される（Ｃ６）。なお、本実施形態では、暗号化手段７６は共通鍵暗号方式の一つであるＤＥＳ方式を用いており、暗号鍵７１をその暗号鍵としている。暗号鍵７１については自分で自分を暗号化する事（暗号化暗号鍵７７Ｋの生成）になる。

【０３３０】そして、指紋データ６５、暗号化秘密鍵７７Ｓ、暗号化暗号鍵７７Ｋ、パスワード６８及び氏名・ＩＤ６９が本人認証データ７８として一つにまとめられ（Ｃ７）、ハードディスク装置１２８等に格納される（Ｃ８）。また、この情報のうち、公開鍵７５は所定の場所に登録されることになる（Ｃ９）。

【０３３１】上述したように、本発明の実施の形態に係

る電子文書の改竄防止システム及び方法は、指紋データを元にして暗号鍵を生成するようにしたので、本人認証を確実なものとすることができるとともに、本人が暗号鍵のデータ自体を知る必要がなく、システムの利用を簡便なものとすることができる。また、暗号鍵そのものが暗号化されていること、秘密鍵が暗号化されている事からたとえ本人認証データ７８を盗まれる事が有っても暗号鍵と秘密鍵の内容を知る事はできず、極めて安全な情報管理を行うことができる。

【０３３２】なお、本実施形態では暗号鍵生成手段７０にパスワードを必要としたが、本発明はこのような場合に限られるものではない。例えば特徴データ６７のみから暗号鍵を生成しても同様の効果が得ることができる。また例えば秘密鍵公開鍵生成手段７３にパスワード６８と乱数発生器７２を必要としていたが、何れか一方が無くても、また両方が無くても同様の効果が得ることが可能である。

【０３３３】さらに、本実施形態では、暗号鍵等の生成に指紋を用いることとしたが、本発明は指紋に限られるものでなく、声紋や虹彩等、本人を特定できるものであれば、種々の生体データを利用することができる。

【０３３４】（第１２の実施の形態）本実施形態は、第１１の実施形態のシステムで登録したシステム使用者に当該システムが使用できるようにする。すなわち、第１～第７の実施形態で説明した電子文書の改竄防止システムにおける各文書認証システム１０１、外部認証システム１０２及び認証文書確認システム１０３を使用するにあたり、そのシステム使用者を確認し、また、各システムで用いられる暗号鍵（秘密鍵、公開鍵等）を使用可能とする手段について説明する。

【０３３５】図２９は本発明の第１２の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９、図１１、図１３、図１５、図１６及び図２７と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２に示す文書認証システム１０１、図３に示す外部認証システム１０２あるいは図６に示す認証文書認証システム１０３が用いられている。本実施形態の独自な機能部分は、文書認証プログラム１３３、外部認証プログラム１３４あるいは認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０３３６】この電子文書の改竄防止システムは、図１に示す文書認証システム１０１、外部認証システム１０２あるいは認証文書確認システム１０３と同様な構成に、以下に各手段が付加されて構成される。なお、以下、文書認証システム１０１の場合を例にとって説明する。

【０３３７】図２９に示す文書認証システム１０１は、正当な使用権限を有する者が電子文書の改竄防止システムを使用したい場合に、パスワード６８及び指紋６５を入力させ、これと第１１の実施形態で生成された本人認証データ７８に予め格納された指紋７８Ｆ、パスワード７８Ｐとにより本人確認を行った後、指紋７８Ｆ、パスワード７８Ｐ及び暗号化暗号鍵７８Ｋから暗号鍵を取出し、さらにこの暗号鍵により暗号化秘密鍵７８Ｓを復号して秘密鍵４を取出して、第１～第７の実施形態の電子文書の改竄防止システムを使用可能な状態にする。

【０３３８】このために文書認証システム１０１には、指紋読取り機６４と、読み取られた指紋６５と本人認証データ７８内の指紋７８Ｆとを照合する照合手段８１と、入力装置１１２から入力されたパスワード６８と、本人認証データ７８内のパスワード７８Ｐとを照合する照合手段８０と、照合手段８０及び８１の結果から本人認証の判定を行う判定ロジック手段８２とが設けられている。さらに、文書認証システム１０１には、判定ロジック手段８２から本人が認証された旨を受けると指紋７８Ｆから特徴データ６７を抽出する特徴抽出手段６６と、特徴データ６７及びパスワード７８Ｐから暗号鍵７１を生成する暗号鍵生成手段７０と、暗号化暗号鍵７８Ｋを暗号鍵７１で復号して暗号鍵８４を取り出す復号手段８３と、暗号鍵７１と暗号鍵８４とを照合して正しく暗号鍵７１が取り出されたことを確認する照合手段８５と、取り出された暗号鍵７１を用い暗号化秘密鍵７８から電子文書の改竄防止システム（図４等）で使用する秘密鍵４を取り出す復号手段８６と、氏名・ＩＤ７８Ｎ等を表示する表示手段７９とが設けられている。

【０３３９】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図２９及び図３０を用いて説明する。

【０３４０】図３０は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０３４１】本動作は生体データ等の入力により本人認証用データに基づいて文書認証システム１０１のシステム起動時等における本人確認及び秘密鍵生成を行う手続きである。

【０３４２】まず、入力装置１１２から本人認証を行う為に名前が入力されると、ハードディスク装置１２８から本人認証データ７８が読み込まれ、表示手段１１１により氏名・ＩＤが表示される。システム使用者は、氏名・ＩＤを確認してパスワード６８を入力する（Ｄ１）。

【０３４３】次に、本人認証データ７８中のパスワード７８Ｐと今入力したパスワード６８とが照合される（Ｄ２）。この照合が一致すれば指紋読み取り機６４で指紋が読取られ、イメージデータである指紋６５が生成される（Ｄ３）。

【０３４４】次に指紋照合手段８１により指紋７８Ｆと読み取った指紋６５とが照合される（Ｄ４）。照合が一致すれば（Ｄ４）、本人認証データ７８から指紋７８Ｆが取り出され特徴抽出手段６６により特徴抽出されて特徴データ６７が生成される（Ｄ５）。ここで読み取った

53

指紋６５を用いずに本人認証データ７８内の指紋７８Ｆを用いるのは、読み取った指紋６５は１ビットも違わずに指紋７８Ｆと一致することは有り得ず、より取るたびに若干の違いを生じるためである。一方、特徴抽出では第８～第１０の実施形態で説明したようにわずかな違いがあっても異なる特徴データとして抽出されるので、第１１の実施形態で取り出した指紋そのものを使用して暗号鍵７１を取り出そうとするものである。

【０３４５】つまり、この特徴データ６７とパスワード７８Ｐが使用され暗号鍵生成手段７０により暗号鍵７１が生成される（Ｄ６）。次に本人認証データ７８から暗号化暗号鍵７８Ｋが取り出されステップＤ６で生成した暗号鍵７１によって復号される（Ｄ７）。

【０３４６】さらにステップＳＴ７で復号した暗号鍵８４とステップＳＴ６で生成した暗号鍵７１が照合手段８５で照合される（Ｄ８）。照合が一致すれば最終的に本人の認証ができたとみなされる。そして、本人認証データ７８から暗号化秘密鍵７８Ｓが取り出され暗号鍵７１を用いた復号手段８６により復号されて秘密鍵４が生成される（Ｄ９）。

【０３４７】こうして電子文書の改竄防止システムが使用可能になり、文書読取り（Ｄ１０）、特徴抽出（Ｄ１１）、秘密鍵４による特徴データの暗号化（Ｄ１２）等といった各実施形態で説明した処理が行われることとなる。

【０３４８】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、システム使用者の指紋６５を読取り、これと本人認証データ７８とを照合するようにしたので、本人認証データ７８から秘密鍵４を取り出す事ができる。ここで、本人認証データ７８内において秘密鍵と暗号鍵は暗号化されて保存されているので、仮に本人認証データを盗まれても秘密鍵と暗号鍵が知られる事はできず非常に安全である。また、暗号鍵は本人認証データの中に保存された指紋７８Ｆから生成されるので確実に同じ暗号データを再現できると共に、暗号データそのものを誰にも知らせる必要が無く極めて安全である。

【０３４９】なお、本実施形態では暗号鍵生成手段７０にパスワードも使用していたが、第１１の実施形態における変形例に対応させて、特徴データ６７だけで暗号鍵を生成するようにしてもよい。本実施形態では指紋を用いて暗号化された鍵について取り扱ったが、本発明は指紋に限られるものでなく、声紋や虹彩等、本人を特定できるものであれば、種々の生体データを利用して本人認証を行うようにしてもよい。

【０３５０】（第１３の実施の形態）本実施形態は、第１１及び第１２の実施形態のシステムにおける指紋読取り機６４で読み取った情報から指紋６５を生成する手段と、指紋６５から特徴抽出を行う特徴抽出手段６６とについて説明する。

54

【０３５１】図３１は本発明の第１３の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９、図１１、図１３、図１５、図１６、図２７及び図２９と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２に示す文書認証システム１０１、図３に示す外部認証システム１０２あるいは図６に示す認証文書認証システム１０３が用いられている。本実施形態の独自な機能部分は、文書認証プログラム１３３、外部認証プログラム１３４あるいは認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０３５２】この電子文書の改竄防止システムは、図１に示す文書認証システム１０１、外部認証システム１０２あるいは認証文書確認システム１０３と同様な構成に、以下に各手段が付加されて構成される。なお、以下、文書認証システム１０１の場合を例にとって説明する。

【０３５３】図３１に示す文書認証システム１０１は、指紋読取り機６４からの指紋原データ８７Ｆから指紋６５を生成する指紋データ抽出手段８７と、指紋６５から特徴データ６７を抽出する特徴抽出手段６６とによって構成されている。

【０３５４】指紋データ抽出手段８７には、境界抽出手段８７Ａと、エンボス手段８７Ｅと、輪郭抽出手段８７Ｌと、２値化手段８７Ｂとが設けられている。

【０３５５】一方、特徴抽出手段６６には、指紋６５からデータ６６ＳＤを切り出す領域切り出し手段６６Ｓと、切り出されたデータ６６ＳＤと予め用意されたパターン６６Ｐとをマッチングさせるマッチング手段６６Ｍと、マッチング手段６６Ｍにより生成された一桁分データ６６Ｄから特徴データ６７を生成する手段（図示せず）とが設けられている。

【０３５６】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図３１、図３２、図３３、図３４及び図３５を用いて説明する。

【０３５７】図３２は指紋データ６５の一例を示す図である。

【０３５８】図３３は指紋データ６５から矩形領域に切り出したデータ６６ＳＤの一例を示す図である。

【０３５９】図３４はマッチングさせるパターンの例の一部分を示した図である。

【０３６０】図３５は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０３６１】図３５において、まず、指紋読み取り機６４により指紋についてのデータが読取られ、指紋原データ８７Ｆが得られる（Ｅ１）。

【０３６２】次に境界抽出手段８７Ａにより指紋データの境界が明確にされ（Ｅ２）、さらにエンボス手段８７

Eにより境界を明確にしたデータのエンボスが取られる（Ｅ３）。次にデータの輪郭抽出が行われ（Ｅ４）、さらに抽出データが２値化されて指紋データ６５を得る（Ｅ５）。図３２にこの様にして得た指紋データ６５のサンプルが示される。

【０３６３】次に、領域切り出し手段６６Ｓによって領域が指定されつつデータ６６ＳＤの切り出しが行われる（Ｅ６）。この様にして切り出したデータのサンプルが図３３に示される。

【０３６４】次にマッチング手段６６Ｍによりデータ６６ＳＤとパターンデータ６６Ｐとのパターンマッチングが行われる（図３５Ｅ７）。図３４にマッチングを行うパターンの一例が示される。パターンマッチチングが成立すると、マッチング手段６６Ｍからマッチングデータを取り出してこれを１桁データ６６Ｄとする（Ｅ８）。

【０３６５】次に、特徴データを生成するのに必要な桁数が指紋６５から読み出されたかが調べられ、まだデータが有る場合にはステップＥ６～Ｅ８が繰り返される（Ｅ９）。必要な桁数を読み終わると（Ｅ９）、１桁データ６６Ｄから生成される特徴データ６７が出力される。

【０３６６】以上により指紋データ６５から暗号鍵を生成する為の特徴データ６７の生成が行われる。

【０３６７】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、指紋データ６５から暗号鍵を生成する為の特徴データ６７を生成することができるので、これを第１１及び第１２の実施形態における本人認証及び秘密鍵復号システムに利用でき、その効果は非常に大きい。

【０３６８】［第１４～第１７の実施形態についての説明］上記第１～第１３の実施形態に説明した発明によれば、文書作成した本人以外に外部認証機関の認証を追加することで、作成した本人による文書改竄をも防止することができ、重要書類を電子化することが可能となる。

【０３６９】しかし、作成した文書に別の作者が一部変更を加えて、新しい文書にする時には、元の作者と新しい作者及び外部認証機関が再び認証を行なう必要がある。

【０３７０】そこで、以下の第１４～１７の実施形態においては、改竄防止の為に認証を行なった電子文書及びデータの変更に関し、オリジナルの作者以外の変更者により電子文書が変更される場合に、当該オリジナル作者の認証を維持しつつ変更電子文書の再認証を可能とする方法及びシステムについて説明する。すなわち以下の実施形態では、複数の作者が複数の時期に渡って作成した電子文書の変更履歴を明らかにしつつ信用性を付与すると共に取り扱い性を高め、従来紙でしかできなかった履歴文書等の変更文書の電子化を実現する。

【０３７１】図３６は本発明の第１４～第１７の実施形態における文書変更を含んだ電子文書の改竄防止システム及び方法の全体的な構成を示す図である。

【０３７２】同図に示すように、公衆回線や専用回線を用いたネットワーク１１００が構成され、当該ネットワークに文書認証システム１１０１や外部認証機関１０９９の外部認証システム１１０２、文書変更認証システム１１０３、認証文書確認システム１１０４が接続されている。

【０３７３】文書認証システム１１０１は、第１～第１３の実施形態で説明した文書認証システム１０１と同様に構成されたシステムである。外部認証システム１１０２は文書認証システム１１０１から認証すべき情報を受信して、認証した結果を返信する。また、外部認証システム１１０２はネットワーク１１００を介して、文書変更認証システム１１０３から認証すべき情報を受信して、認証した結果を返信する。

【０３７４】文書認証システム１１０１、文書変更認証システム１１０３、認証文書確認システム１１０４は複数存在してよく、異なった使用者によって使用される。

【０３７５】また、文書認証システム１１０１、外部認証システム１１０２、文書変更認証システム１１０３、及び認証文書確認システム１１０４は、ワークステーションやパーソナルコンピュータなどの計算機に表示装置、入力装置、あるいは例えば指紋読取装置、スキャナ装置などを付加したものであり、基本的には動作プログラムが異なる事で異なる各機能を実現する。従って、文書認証システム１１０１、文書変更認証システム１１０３、認証文書確認システム１１０４は一つの計算機上に構成される場合も有る。

【０３７６】さらに、文書変更認証システム１１０３及び外部認証システム１１０２とを同一計算機、あるいはＬＡＮ等で接続される計算機上に構成させ、外部認証機関において、認証作業の全てを行うようにする事も可能である。

【０３７７】本発明に関わる電子文書の変更認証システム及び方法は、これらの文書認証システム１１０１、外部認証システム１１０２、文書変更認証システム１１０３及び認証文書確認システム１１０４を適宜組み合わせ、あるいはその一部機能を適宜組み合わせて成るものである。さらに本明細書では、便宜上、第１～第１３の実施形態と第１４～第１７の実施形態とにわけて説明しているが、両実施形態グループに属する各システムを適宜組み合わせ、あるいはその一部機能を適宜組み合わせ又組み込むことも可能である。

【０３７８】また、上記場合はネットワークを介した情報の瞬時転送を前提とした場合を説明しているが、図３６に示す様にフロッピーディスク等の記録媒体９７，９８を介して文書変更認証システム１１０１～外部認証システム１１０２間、あるいは文書認証システム１１０１～文書変更認証システム１１０３間、文書変更認証システム１１０３～認証文書確認システム１１０４間で必要

情報の交換を行う事も可能である。

【０３７９】全体的には以上のシステム構成を有する文書変更を含んだ電子文書の改竄防止システム及び方法について、対応する第１４～第１７の実施形態を説明する。

【０３８０】(第１４の実施の形態)本実施形態は改竄を防止できる電子文書の変更システム及び方法に関するものである。

【０３８１】図３７は本発明の第１４の実施形態に係る文書変更を含んだ電子文書の改竄防止システムに適用される文書変更認証システムのハードウェア構成例を示すブロック図である。

【０３８２】文書変更認証システム１１０３は、計算機１１１０に、表示装置１１１１、入力装置１１１２、印刷装置１１１３、外部記憶装置１１１４、指紋読み取り機１０６４、スキャナ１１１５が接続されてなっている。

【０３８３】この文書変更認証システム１１０３の上記ハードウエア構成は、図２に示す文書認証システム１０１と同様なものであり、ここでは説明を省略する。すなわち、計算機１１１０、表示装置１１１１、入力装置１１１２、印刷装置１１１３、外部記憶装置１１１４、指紋読み取り機１０６４、スキャナ１１１５が、それぞれ計算機１１０、表示装置１１１、入力装置１１２、印刷装置１１３、外部記憶装置１１４、指紋読み取り機６４、スキャナ１１５に対応する。

【０３８４】また、計算機１１１０内の構成についても同様であり、文書変更認証システム１１０３の各構成要素１１１６～１１３３が、文書認証システム１０１の各構成要素１１６～１３３に対応している。

【０３８５】ただし、ハードディスク装置１１２８やＲＡＭ１１１９等に格納されるソフトウエア的要素のうち、文書変更認証システム１１０３に対応する部分は本実施形態独自のものとなる。すなわちプログラム格納部１１３０は文書変更認証システム１１０１を実現するプログラム等を格納し、また、ＲＡＭ１１１９は、文書変更認証プログラム１１３３を格納する。なお、第１実施形態と同様に、この文書変更認証プログラム１１３３は、ハードディスク装置１１２８のプログラム格納部１１３０から呼び出され、ＲＡＭ１１１９内に格納される。

【０３８６】また、ＣＰＵ１１１７は、ＲＡＭ１１１９内の文書変更認証プログラム１１３３に従って各部を制御し、文書変更認証システム１１０３を実現する。

【０３８７】本実施形態及び以下の各実施形態における処理説明図や流れ図などに表現される各手段（各処理）あるいは図示しない各手段（各処理）は、主として文書変更認証プログラム１１３３に従うＣＰＵ１１１７の動作による機能実現手段である。

【０３８８】次に外部認証システムのハードウェア構成について説明する。

【０３８９】図３８は本実施形態の文書変更を含んだ電子文書の改竄防止システムに適用される外部認証システムのハードウェア構成例を示すブロック図であり、図３７と同一部分には同一符号を付してその説明を省略する。

【０３９０】外部認証システム１１０２は、文書変更認証システム１１０３と同様な計算機システムから構成される。文書変更認証システム１１０３との相違点は、ハードディスク装置１１２８のプログラム格納部に格納される動作プログラムである。この動作プログラムが呼び出され、ＲＡＭ１１１９内に外部認証プログラム１１３４として格納される。ＣＰＵ１１１７は、この外部認証プログラムに従って各部を制御し、外部認証システム１１０２が実現される。また、ソフトウェア資源（特に外部認証プログラム１１３４）とハードウェア資源とが結合して機能実現手段が構成される点も文書変更認証システム１１０３の場合と同様である。

【０３９１】次に図３９及び図４０を用いて文書変更を含んだ電子文書の改竄防止システムの各構成について説明する。

【０３９２】図３９及び図４０は本実施形態の文書変更を含んだ電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図である。

【０３９３】この文書変更を含んだ電子文書の改竄防止システムは文書変更認証システム１１０３と外部認証システム１１０２とから構成されている。

【０３９４】まず図３９の構成を説明する。

【０３９５】文書変更認証システム１１０３は、分離手段１００５と、変更者#nの変更及び認証手段１００６と、結合手段１００９とから構成され、変更履歴付電子文書１００１から変更履歴付電子文書１０１１を生成するようになっている。

【０３９６】ここで変更履歴付電子文書１００１は、過去に変更があった電子文書あるいは過去に変更はないがこれから変更を施す電子文書であって、認証付き原電子文書１００２と、1回目変更からn-1回目変更までの認証付き変更箇所データ１００３と、n-1回目の認証付き変更電子文書１００４とから構成されている。

【０３９７】分離手段１００５は、変更履歴付電子文書１００１を各構成要素に分離する。

【０３９８】変更者#nの変更及び認証手段１００６は、n-1回目の認証付き変更電子文書１００４を外部認証システム１０２に送出し、その応答結果に基づき、変更者#nによるn回目変更箇所１００７、変更者#n によるn回目変更電子文書１００８を出力する。

【０３９９】結合手段１００９は、認証付き原電子文書１００２と、1回目変更からn-1回目変更までの認証付き変更箇所データ１００３と、変更者#n によるn回目変更箇所１００７と、変更者#n によるn回目変更電子文書１

００８とを結合して変更履歴付電子文書１０１１を生成する。ここで、変更履歴付電子文書１０１１は、認証付き原電子文書１００２と、1回目からn回目までの変更箇所１０１０と、n回目変更電子文書１００８とから構成される。

【０４００】次に、図４０を用いて変更者#nの変更及び認証手段１００６の詳細構成及び外部認証システム１１０２の概略構成を説明する。

【０４０１】変更者#nの変更及び認証手段１００６は、文書変更手段１０２１と、差分抽出手段１０２３と、変更者認証手段１０２５Ａ，１０２５Ｂと、結合手段１０２８とを備えている。

【０４０２】文書変更手段１０２１は、変更電子文書１０２０を変更者#nによる変更電子文書１０２２に変換する。差分抽出手段１０２３は、変更電子文書１０２０と変更者#nによる変更電子文書１０２２との差分を抽出し、この差分データから構成されるn回目変更箇所１０２４を生成する。

【０４０３】変更者認証手段１０２５Ａ，１０２５Ｂは、それぞれ変更者の認証データで変更電子文書１０２２、変更箇所１０２４を認証し、変更者認証データ１０２６Ａ、変更者差分認証データ１０２６Ｂを出力する。

【０４０４】結合手段１０２８は、認証データ１０２７と変更者認証データ１０２６Ａとを結合し、結合認証データ１０２９を出力する。

【０４０５】特に図示しないが、変更者#nの変更及び認証手段１００６は、さらに、n-1回目の認証付き変更電子文書１００４から変更電子文書１０２０及び認証データ１０２７を取り出す手段と、変更箇所１０２４と認証データ１０３２Ｂを結合して変更箇所１００７を生成する手段と、変更電子文書１０２２と認証データ１０３２Ａとを結合して変更電子文書８を生成する手段とを備えている。

【０４０６】一方、外部認証システム１０２は、認証データ１０２９に対し、外部認証機関による認証を行って認証データ１０３１Ａを生成する外部認証手段１０３０Ａと、変更者差分認証データ１０２６Ｂに対し、外部認証機関による認証を行って認証データ１０３１Ｂを生成する外部認証手段１０３０Ｂとを備えている。

【０４０７】なお、認証データ１０２９及び変更者差分認証データ１０２６Ｂは、文書変更認証システム１１０３から外部認証システム１１０２に送信され、その認証結果１０３１Ａ，１０３１Ｂが外部認証システム１１０２から返信されるようになっている。

【０４０８】次に、図４１を用いて、変更者#nの変更及び認証手段１００６の変更者認証手段１０２５Ａについて説明する。

【０４０９】図４１は変更者#nの変更及び認証手段における変更者認証手段の構成を示す図である。

【０４１０】変更認証手段１０２５Ａは、変更者#nの秘密鍵１０２５Ａ－３及び見出し１０２６Ａ－Ｈを保持するとともに、特徴抽出手段１０２５Ａ－１及び暗号化手段１０２５Ａ－４を備えている。

【０４１１】特徴抽出手段１０２５Ａ－１は、変更電子文書２２から特徴データ１０２５Ａ－２を抽出して暗号化手段１０２５Ａ－４に引き渡す。暗号化手段１０２５Ａ－４は、特徴データ１０２５Ａ－２を変更者#nの秘密鍵１０２５Ａ－３で暗号化して暗号データ１０２６Ａ－Ｄを生成する。

【０４１２】変更認証手段１０２５Ａは、暗号データ１０２６Ａ－Ｄに見出し１０２６Ａ－Ｈを付加して、変更者の認証データ１０２６Ａを生成する。

【０４１３】なお、変更者認証手段１０２５Ｂについては特に図示しないが、変更者認証手段１０２５Ａと同様に構成される。

【０４１４】図４２は外部認証システムにおける外部認証手段の構成を示す図である。

【０４１５】外部認証手段１０３０Ａは、認証実行ＩＤを含む外部認証データ１０３０Ａ－Ａ及び外部認証機関の秘密鍵１０３０Ａ－２を保持するとともに、結合手段１０３０Ａ及び暗号化手段１０３０Ａ－３を備えている。

【０４１６】文書変更認証システム１１０３から送信される結合認証データ１０２９は、見出し１０２６Ａ－Ｈ及び暗号データ１０２６Ａ－Ｄからなる変更者の認証データ１０２６Ａと、認証データ１０２７とから構成されている。この結合認証データ１０２９は、外部認証手段１０３０Ａにて、見出し１０３１Ａ－Ｈと、暗号データ１０２６Ａ－Ｄ及び認証データ１０２７とに分離される。

【０４１７】暗号化手段１０３０Ａは、外部認証データ１０３０Ａ－Ａと、暗号データ１０２６Ａ－Ｄ及び認証データ１０２７とを結合し、暗号化手段１０３０Ａ－３は、この結合結果を秘密鍵１０３０Ａ－２で暗号化する。

【０４１８】外部認証手段１０３０Ａにより最終的に生成される外部認証機関の認証データ１０３１Ａは、見出し１０３１Ａ－Ｈと、暗号化手段１０３０Ａ－３により暗号化された暗号データ１０３１Ａ－Ｄからなる。

【０４１９】なお、外部認証手段１０３０Ｂについては特に図示及び説明しないが、これは外部認証手段１０３０ＡにおけるＡとＢとを読み替えたものと同じである。

【０４２０】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図３９～図４３を用いて説明する。

【０４２１】図４３は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０４２２】まず、文書変更認証システム１１０３において、変更履歴付電子文書１００１の読み込みが行われる（ＳＳ１）。

【０４２３】次に、分離手段１００５によって、変更履歴付原電子文書１００２、変更履歴付n-1回目までの変更箇所１００３及び変更履歴付n-1回目の変更電子文書１００４に分離される（ＳＳ２）。

【０４２４】次のステップＳＳ３からＳＳ７までの処理は変更及び認証手段１００６によって行われる。すなわち、図３９及び図４０に示すように、変更者#n(以下、複数存在し得る同種類の構成やデータには、場合により#1、#2、..あるいは第1の、第2の、..と記して区別する)が使用する変更及び認証手段6により、取り出されたn-1回目の認証付き変更電子文書１００４が変更され及び変更者#nの認証が行われ、変更者#nの認証データが外部認証システム１１０２に送信される。

【０４２５】具体的にはまず、n-1回目の認証付き変更電子文書１００４から、n-1回目変更電子文書１０２０が取り出される。さらに。変更者#nの入力操作で変更手段１０２１により、n-1回目の変更電子文書１０２０が変更され、n回目の変更電子文書１０２２が生成される（ＳＳ３）。

【０４２６】次に、差分抽出手段１０２３により、n-1回目の変更電子文書１０２０とn回目の変更電子文書１０２２と差分の抽出が行なわれ、n回目変更箇所１０２４の差分データが抽出される（ＳＳ４、図４０）。

【０４２７】この処理（ＳＳ４）は、次にようにしてなされる。すなわち各電子文書は詰まる所0と1から構成されるバイナリデータである。差分抽出手段１０２３は、これらバイナリデータの差分を抽出して、n回目変更箇所データ１０２４を出力する。これによりn回目変更箇所データ１０２４には、n-1回目変更電子文書１０２０とn回目変更電子文書１０２２の間でどの場所でどのデータが削除されたか、どの場所でどのデータが挿入されたか、どの場所でどのデータが入れ替えられたかの情報が保存される。

【０４２８】次に、変更者#nによる文書変更完了後の認証行われ、n回目変更電子文書１０２２とn回目変更箇所１０２４からそれぞれn回目変更電子文書の変更者認証データ１０２６Ａとn回目変更箇所の変更者認証データ１０２６Ｂが生成される（ＳＳ５、図４０）。

【０４２９】すなわちn回目変更電子文書１０２２が変更者認証手段１０２５Ａに与えられ、n回目変更者認証データ１０２６Ａが生成される。このためにまず、特徴抽出手段１０２５Ａ－１によってn回目変更変更電子文書１０２２の特徴データ１０２５Ａ－２が抽出される（図４１）。この特徴データ１０２５Ａ－２はn回目変更変更電子文書１０２２のどの1ビットが変化してもその値が異なった値となる様な電子文書自体の特徴を示すデータである。一方、見出し１０２６Ａ－Ｈは、特徴データ１０２５Ａ－２がn回目変更変更電子文書１０２２に属するデータである事をわかるようにする為に追加されるデータである。

【０４３０】次に、特徴データ１０２５Ａ－２は、変更者#nの秘密鍵１０２５Ａ－３を使用して暗号化手段１０２５Ａ－４で暗号化され、暗号データ１０２６Ａ－Ｄとして出力される。変更者#nの秘密鍵１０２５Ａ－３は、文字通り、変更者#n以外には知らせない様にした鍵で、変更者#nの公開鍵と対を成すものである。見出し１０２６Ａ－Ｈと暗号データ１０２６Ａ－Ｄとは対応しており、まとめて変更者認証データ１０２６Ａとして出力される。

【０４３１】同様にして、変更者認証手段１０２５Ｂによってn回目変更箇所データ１０２４から特徴が抽出され、 n回目変更者差分認証データ１０２６Ｂが生成される。

【０４３２】次に、n-1回目の認証付き変更電子文書１００４から取り出したn-1回目の変更電子文書認証データ１０２７と、n回目の変更電子文書の変更者認証データ１０２６Ａと結合手段２８によりが結合され、n回目の結合認証データ１０２９が生成される（ＳＳ６、図４０）。

【０４３３】次に、 n回目の結合認証データ１０２９とn回目変更箇所の変更者認証データ１０２６Ｂとが文書変更認証システム１１０３の通信装置１１２９を介してネットワーク１１００を通り外部認証システム１１０２に送信される（ＳＳ７）。

【０４３４】次のステップＳＳ８からＳＳ１０までの処理は外部認証システム１１０２において行われる。

【０４３５】まず、外部認証システム１１０２は文書変更認証システム１１０３から送られたn回目変更文書の変更者結合認証データ１０２９とn回目変更者差分認証データ１０２６Ｂを受信する（ＳＳ８）。

【０４３６】次に、外部認証システム１１０２において、送られたn回目の結合認証データ１０２９とn回目変更箇所の変更者認証データ１０２６Ｂとがそれぞれ外部認証手段１０３０Ａ、１０３０Ｂにより認証され、それぞれ認証データ１０３１Ａ、１０３１Ｂが生成される（ＳＳ９、図４０）。以下にこの処理を説明する。

【０４３７】このためにまず、外部認証手段１０３０Ａによって、n回目変更文書の変更者結合認証データ１０２９から見出し１０３１Ａ－Ｈが取り出される。引き続いて、残りの暗号データ/認証データ１０２６Ａ－Ｄ／１０２７が結合手段１０３０Ａ－１に与えられる（図４２）。

【０４３８】この暗号データ/認証データ１０２６Ａ－Ｄ／１０２７に、外部認証機関の外部認証データ１０３０Ａ－Ａ（認証実行ＩＤ）が結合手段１０３０Ａ－１により結合される。なお、この認証実行識別情報としての認証実行ＩＤは原則として認証毎に異なるものであり、どの認証に対してとの認証実行ＩＤを付与したかは、外部認証機関１０９９に保存される。

【０４３９】次に、この結合データが、外部認証機関の

秘密鍵１０３０Ａ－２を用いて暗号化手段１０３０Ａ－３により暗号化され、暗号データ１０３１Ａ－Ｄが生成される。

【０４４０】ここで、外部認証データ１０３０Ａ－Ａは文書変更認証システム１１０３が認証を要求してきたデータに対して第三者である外部認証機関が認証した事を示す情報であり、認証した日付データが含まれる。見出し１０３１Ａ－Ｈと暗号データ１０３１Ａ－Ｄは、データの関係付けが行われ、n回目変更電子文書認証データ１０３１Ａとして出力される。

【０４４１】同様に、変更者差分認証データ１０２６Ｂも外部認証手段１０３０Ｂによって外部認証が与えられ、n回目差分認証データ１０３１Ｂとして出力される。この場合の外部認証手段１０３０Ｂの処理については、図４２のAをBと読み替えて説明を行なう。

【０４４２】すなわち外部認証手段１０３０Ｂでは、n回目変更文書の変更者結合認証データ１０２９を受け取る代わりに、 n回目変更者差分認証データ１０２６Ｂからデータを受け取ると、見出し１０３１Ｂ－Ｈを取り出して、残りの暗号データ１０２６Ｂ－Ｄが結合手段１０３０Ｂ－１に与えられる。前記暗号データ１０２６Ｂ－Ｄに外部認証機関の外部認証データ１０３０Ｂ－Ａが結合手段１０３０Ｂ－１により結合され、外部認証機関の秘密鍵１０３０Ｂ－２を用いて暗号化手段１０３０Ｂ－３により暗号化され暗号データ１０３１Ｂ－Ｄを生成する。ここで、外部認証データ１０３０Ｂ－Ａは文書変更認証システム１１０３が認証を要求してきたデータに対して第三者である外部認証機関が認証した事を示す情報であり、認証した日付データが含まれる。見出し１０３１Ｂ－Ｈと暗号データ１０３１Ｂ－Ｄはn回目差分認証データ１０３１Ｂとしてデータの関係付けが行われる。

【０４４３】こうして生成されたn回目変更電子文書認証データ１０３１Ａ及びn回目差分認証データ１０３１Ｂは、外部認証システム１１０２の通信装置１１２９を介してネットワーク１１００を通り文書変更認証システム１１０３に送信される（ＳＳ１０）。

【０４４４】文書変更認証システム１１０３においては、外部認証システム１１０２から送られたデータを認証データ１０３２Ａ、１０３２Ｂとして受信し、この受信データを変更及び認証手段１００６に与える（ＳＳ１１）。

【０４４５】次に、変更及び認証手段１００６において、n回目変更電子文書認証データ１０３１Ａはn回目変更電子文書１０２２との関係付けが行われ、n回目の認証付き変更電子文書１００８が生成され出力される。同様に、n回目差分認証データ１０３１Ｂはn回目変更箇所データ１０２４との関係付けが行われ、n回目の認証付き差分認証データ１００７が生成され出力される（ＳＳ１２、図４０）。

【０４４６】次に、変更箇所データ１００７は、結合手段１００９によって、1回目変更からn-1回目変更までの認証付き変更箇所データ１００３と結合され、各々関係付けのなされた1回目からｎ回目までの認証付き変更箇所データ１０１０となる。さらに、結合手段１００９により、認証付き原電子文書１００２、1回目からｎ回目までの認証付き変更箇所データ１０１０およびｎ回目認証付き変更電子文書１００８が関係付けられたn回目変更履歴付電子文書１０１１が生成される（ＳＳ１３、図３９）。

【０４４７】なお、n+1の変更を実施する時には、変更履歴付電子文書１００１をn回目の変更履歴付き電子文書とすると、 n+1回目の変更履歴付き電子文書が変更履歴付電子文書１０１１として得られる。

【０４４８】上述したように、本発明の実施の形態に係る変更電子文書の改竄防止システム及び方法は、変更者により電子署名された変更文書を外部認証機関が認証する手順を踏んで追加的な認証を行うようにしたので、外部認証機関の認証日付にはまさしく変更者が変更文書を作成していた事が証明される。また、電子署名が無い場合であっても文書変更者本人の秘密鍵で特徴データの暗号化がなされ、これに対応する公開鍵で復号化される事になるので、何れにしても文書変更者の変更になる文書である事が認証される。

【０４４９】また、変更文書本体の改竄を行なうと改竄後の文書から抽出されるべき特徴データが変化し、先に認証用に抽出された特徴データ１０２５Ａ－２と異なるものになる事によって、変更文書本体の改竄の事実が検出できる。一方先に認証用に抽出された特徴データ１０２５Ａ－２は外部認証機関の認証データ１０３０Ａ－Ａとともに認証機関の秘密鍵１０３０Ａ－２で暗号化されているので、認証付き変更電子文書１００８に付されている認証データ１０３２Ａの改竄は不可能である。従って、たとえ本人であっても外部認証後には文書改竄が不可能になる。

【０４５０】これにより裁判の場で文書の正当性が証明できる、証拠能力のある変更電子文書が生成できるため、従来紙で保存していた重要文書や、証拠書類を電子化する事が可能となる。また、従来の紙の文書でも改竄の有無を判定するには高度な技術が必要とされたが、本発明になる電子文書の改竄防止システムでは電子的な手順を踏むだけで改竄の有無を確認できるので、改竄の有無を容易に証明できる。

【０４５１】さらに電子化により保管場所が削減できると共に、遠隔地への文書伝送が瞬時に行なえる様になり、コンピュータによる検索が行なえるようになる。こうして、商取引の信用向上、取り引きの迅速化を図る事ができる。

【０４５２】また、本実施形態の変更文書改竄防止システムでは、文書変更認証システム１１０３や外部認証システム１１０２に於いて伝送データの暗号化が行われる

65

ので、ネットワーク１１００として公衆回線を用いても安全である。

【０４５３】さらに、本実施形態の変更文書改竄防止システムでは、文書変更認証システム１１０３と外部認証システム１１０２との間でやり取りされるデータは文書データではなく、文書データの特徴（差分データ等）であるので、文書データそのものの内容はネットワーク１１００や外部認証システム１１０２に流す必要が無く、文書データの秘密を保つ事ができる。

【０４５４】さらに、外部認証機関が認証した外部認証データを元の変更電子文書と変更箇所に結合して認証付きの変更履歴付文書１０１１の形で管理するようにしたので、電子文書を保存する時の扱いが楽になる。

【０４５５】（第１５の実施の形態）本実施形態では、第１４の実施形態で認証した認証付き変更電子文書１０１１が真正なものである事を確認し、また外部認証機関の付した認証日付などの認証情報を取り出すシステムについて説明する。

【０４５６】この変更電子文書の改竄防止システムは、図３６に示した認証文書確認システム１１０４として構成されるものである。

【０４５７】図４４は本発明の第１５の実施の形態に係る変更電子文書の改竄防止システムに適用される認証文書確認システムのハードウェア構成例を示すブロック図であり、図３７と同一部分には同一符号を付してその説明を省略する。

【０４５８】認証文書確認システム１１０４は、文書変更認証システム１１０３と同様な計算機システムから構成される。文書変更認証システム１１０４との相違点は、ハードディスク装置１１２８のプログラム格納部１１３０に格納される動作プログラムである。この動作プログラムが呼び出され、ＲＡＭ１１１９内に認証文書確認プログラム１１３５として格納される。ＣＰＵ１１１７は、この認証文書確認プログラム１１３５に従って各部を制御し、認証文書確認システム１１０４が実現される。また、ソフトウェア資源とハードウェア資源とが結合して機能実現手段が構成される点も文書変更認証システム１１０３の場合と同様である。

【０４５９】次に図４５～図４７を用いて電子文書の改竄防止システムの機能構成について説明する。

【０４６０】図４５は本実施形態の変更電子文書の改竄防止システムに適用される認証文書確認システムの機能構成ならびに処理流れの一例を示す図であり、図３９と同一部分には同一符号を付して説明を省略する。

【０４６１】同図において、認証確認の対象となる変更電子文書１０１１Ｂは、原電子文書１００２Ｂと、変更電子文書１００８Ｂと、1回目からn回目までの変更箇所１００７Ｂ#1～１００７Ｂ#n-1及び１００７Ｂとからなり、これは第１４の実施形態における変更電子文書１０１１に対応している。

66

【０４６２】一方、認証文書確認システム１１０４には、n回目の認証確認手段１０４０と、n-1回目の認証確認手段１０４０#n-1と、日付確認手段１０４１，１０４１#n-1と、同一性判定手段１０４２，１０４２#n-1とが設けられる。さらに、認証文書確認システム１１０４には、繰返し部分となる認証確認手段１０４０と同様な認証確認手段１０４３と、第１～第１３の実施形態におけるものと同様な認証確認手段１０４４，日付確認手段１０４５及び同一性判定手段１０４６とが設けられている。

【０４６３】また、認証文書確認システム１１０４には、変更履歴付電子文書１０１１Ｂから認証付き原電子文書１００２Ｂと、1回目変更からn回目変更までの認証付き変更箇所データ１００７Ｂ#1，１００７Ｂ#2，…１００７Ｂ#n-1，１００７Ｂと、n回目の認証付き変更電子文書１００８Ｂとを取り出し、認証データと文書データと変更箇所データとに分解する手段（図示せず）が設けられている。

【０４６４】次に図４６及び図４７を用いて認証文書確認システム１１０４を構成する認証確認手段の各機能構成について説明する。

【０４６５】図４６は認証確認手段１０４０の詳細構成を示す図であり、図４７は認証確認手段１０４０#n-1の詳細構成を示す図である。

【０４６６】認証確認手段１０４０は、n回目の認証付き変更電子文書１００８Ｂの認証を確認する認証確認手段１０４０Ａと、n回目の認証付き変更箇所１００７Ｂの認証を確認する認証確認手段１０４０Ｂとから構成される。

【０４６７】認証確認手段１０４０Ａにおいては、認証データ１４０１Ａ、外部認証機関１０９９の公開鍵１４０２Ａ、見出しを含む変更者結合認証データ１４０４Ａ、変更者認証データ１４０６Ａ、以前の認証データ１４０７Ａ、変更者の公開鍵１４０８Ａ、特徴データ１４１０Ａ及び特徴データ１４１２Ａが保持されている。また、復号化手段１４０３Ａ、分離手段１４０５Ａ、復号化手段１４０９Ａ、特徴抽出手段１４１１Ａ及び照合手段１４１３Ａが設けられている。

【０４６８】ここで、見出しを含む変更者結合認証データ１４０４Ａは、見出し１４０１Ａ－Ｈと暗号データ１４０１Ａ－Ｄから構成される。また、見出しを含む変更者結合認証データ１４０４Ａは、見出し１４０４Ａ－Ｈと変更者結合認証データ１４０４Ａ－Ｄとから構成され、変更者結合認証データ１４０４Ａ－Ｄはさらに変更者結合認証データ１４０４Ａ－Ｄ１と外部認証機関１０９９の認証データ１４０４Ａ－Ｄ２とから構成される。以前の認証データ１４０７Ａは見出しと認証データ本体とから構成される。

【０４６９】一方、認証確認手段１０４０Ｂにおいては、認証データ１４０１Ｂ、外部認証機関１０９９の公

開鍵１４０２Ｂ、見出しを含む変更者認証データ１４０４Ｂ、変更者の公開鍵１４０８Ｂ、特徴データ１４１０Ｂ、特徴データ１４１２Ｂが保持されている。また、復号化手段１４０３Ｂ、復号化手段１４０９Ｂ、特徴抽出手段１４１１Ｂ、照合手段１４１３Ｂが設けられている。

【０４７０】ここで、見出しを含む変更者認証データ１４０１Ｂは見出し１４０１Ｂ－Ｈと暗号データ１４０１Ｂ－Ｄから構成される。見出しを含む変更者認証データ１４０４Ｂは見出し１４０４Ｂ－Ｈと変更者認証データ１４０４Ｂ－Ｄとから構成され、変更者認証データ１４０４Ｂ－Ｄはさらに変更者認証データ１４０４Ｂ－Ｄ１と外部認証機関１０９９の認証データ１４０４Ｂ－Ｄ２とから構成される。

【０４７１】次に図４７を用いて認証確認手段１０４０#n-1を説明する。

【０４７２】認証確認手段１０４０#n-1は、n-1回の認証データ１０２７の認証を確認する認証確認手段１０４０Ａと、n-1回目の認証付き変更箇所１００７Ｂ#n-1の認証を確認する認証確認手段１０４０Ｂとから構成される。

【０４７３】ここで、図４７における認証確認手段１０４０Ａ及び１０４０Ｂと図４６における認証確認手段１０４０Ａ及び１０４０Ｂとは同一の手段を使用するが、n-1回以前の認証データ１０２７の認証確認で使用しない機能は図示を省略している。

【０４７４】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図４５～図５０を用いて説明する。

【０４７５】この認証文書確認システム１１０４においては、変更履歴付電子文書１０１１Ｂ内のn回目の認証付き変更電子文書１００８Ｂからスタートしてn回目の側から原文書の方向に向って順次認証の確認が繰返され、原文書と最終文書、および全ての変更箇所の電子文書の同一性確認が行われる。また、認証データから取り出された外部認証データから外部認証機関１０９９による認証の事実及びその認証日付１０４５，１０４１#1，１０４１#2，…１０４１#n-1，１０４１が確認される。

【０４７６】図４８は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０４７７】同図においてまず、まず、外部記憶装置１１１４、ハードディスク装置１１２８から、あるいはネットワーク１１００を介して変更履歴付電子文書１０１１Ｂが読み込まれる（ＴＴ１）。この変更履歴付電子文書１０１１Ｂからは、認証付き原電子文書１００２Ｂと、1回目変更からn回目変更までの認証付き変更箇所データ１００７Ｂ#1，１００７Ｂ#2，…１００７Ｂ#n-1，１００７Ｂと、n回目の認証付き変更電子文書１００８Ｂとが取り出され、さらに認証データと文書データ、変

更箇所データに分解される(ＴＴ２)。

【０４７８】次に、文書変更回数Ｎが最終の変更回数n回に設定され、認証確認初回フラグが設定される（ＴＴ３）。

【０４７９】ここで、初回の認証確認かどうかが判断される（ＴＴ５）。初回の場合にはＮ回目変更文書データ１００８Ｂの認証データ、Ｎ回目変更文書１００８Ｂの文書データ、Ｎ回目変更箇所１００７Ｂの変更認証データ、及びＮ回目変更箇所１００７Ｂの変更箇所データが認証確認手段１０４０に読み込まれる（ＴＴ６）。

【０４８０】続いて認証確認手段１０４０により認証確認が実行され、認証データ１０２７が出力され、少なくとも外部認証機関の日付と認証実行ＩＤを含んだ日付認証データ１０４１が生成される（ＴＴ８）。

【０４８１】一方、ステップＴＴ５で初回でない場合には、Ｎの数に応じてn-1回目変更箇所１００７Ｂ#N-1から1回目変更箇所１００７Ｂ#1までのどれかが認証確認手段１０４０に読み込まれる（ＴＴ７）。

【０４８２】続いて認証確認手段１０４０#n-1，１０４０#n-2…により認証確認が実行され、認証データ１０２７が出力され、日付認証データ１０４１#n-1，１０４１#n-2…が生成される（ＴＴ８）。ここで認証確認手段１０４１#n-1，１０４１#n-2…は同じ認証確認手段が繰り返し呼び出される。

【０４８３】ここで、n回目、n-1回目 及びn-2回目から1回目におけるステップＴＴ８の認定内容について簡単に説明する。

【０４８４】すなわちまず、n回目の認証付き変更電子文書１００８Ｂ及びn回目の認証付き変更箇所１００７Ｂの認証確認が認証確認手段１０４０により行われる。これにより、n-1回目までの認証データ１０２７が出力され、外部認証機関の認証日付１０４１が出力される。さらに、n回目変更電子文書１００８Ｂとn回目認証付き変更箇所１００７Ｂが、変更履歴付電子文書１０１１のn回目変更電子文書１００８とn回目認証付き変更箇所１００７と同一であるか否かの同一性判定１０４２が行われる。

【０４８５】また、 n-1回目の認証付き変更箇所１００７Ｂ#n-1の認証確認は、認証確認手段１００４#n-1により行われる。すなわち、n-2回目までの認証データ１０２７#n-1が出力され、外部認証機関の認証日付１０４１#n-1が出力される。さらに、n-1回目認証付き変更箇所１００７Ｂ#n-1が変更履歴付電子文書１０１１のn-1回目認証付き変更箇所１００７#n-1と同一であるか否かの同一性判定１０４２#n-1が行われる。

【０４８６】また、同様に認証確認手段１０４３により、n-2回目から1回目の認証付き変更箇所１００７Ｂ#1から１００７Ｂ#n-2に基づき、それぞれの回の認証データ及び外部認証機関の認証日付が出力される。さらに、認証付き変更箇所１００７Ｂ#1…１００７Ｂ#n-2が変更

履歴付電子文書１０１１の認証付き変更箇所１００７#1…１００７#n-2と同一であるか否かの同一性判定が行われる。

【０４８７】以上の何れかの認証確認（ＴＴ8）が実行された後、認証実行ＩＤの不一致または同一性判定手段１０４２の判定が否の場合（ＴＴ９）は、Ｎ回目文書の不一致が表示装置１１１１に表示されて終了する。なお、外部記憶装置１１１４に出力したり、ハードディスク装置１１２８に出力したり、ネットワーク１１００に出力したりして終了してもよい（ＴＴ１０）。

【０４８８】一方、認証実行ＩＤが一致しかつ同一性判定手段１０４２の判定が真の場合（ＴＴ９）には、認証確認初回フラグがクリアされ、変更回数Ｎを1減じる（ＴＴ１１）。

【０４８９】次に変更回数Ｎが１かどうかが判定され（ＴＴ１２）、Ｎが1より大きい場合にはステップＴＴ４に戻り、初回の認証確認かどうかが判断されて（ＴＴ５）、ステップＴＴ５～ステップＴＴ１２が繰り返される。

【０４９０】一方、変更回数Ｎが1の場合には（ＴＴ１２）、認証付き原電子文書１００２Ｂの認証データと文書データが認証確認手段１０４４に読み込まれる（ＴＴ１３）。なお、ここで与えられる認証データは認証確認手段１０４３から出力されるものであり、文書データは、認証付き原電子文書１００２Ｂから認証部分を除いたものである。

【０４９１】続いて、認証確認手段１０４４により認証確認が実行され、原文書の外部認証機関の日付認証データ１０４５が出力され、原電子文書１００２Ｂと原電子文書１００２とが同一であるか否かの同一性判定１０４６が行われる（ＴＴ１４）。なお、認証確認手段１０４４により認証確認処理は、先の実施形態におけるものと同様であるので説明を省略する。

【０４９２】ここで同一性判定手段１０４６の判定が否の場合（ＴＴ１５）には、原電子文書１００２Ｂが不一致である旨が表示装置１１１１に表示されて終了する。なお、外部記憶装置１１１４に出力したり、ハードディスク装置１１２８に出力したり、ネットワーク１１００に出力したりして終了してもよい（ＴＴ１６）。

【０４９３】一方、同一性判定手段１０４６の判定が真の場合（ＴＴ１５）には、文書一致である旨と、原電子文書の作成日付からn回目変更文書までの変更日付とが表示装置１１１１に表示されて終了する。また、外部記憶装置１１１４に出力したり、ハードディスク装置１１２８に出力したり、ネットワーク１１００に出力したりして終了してもよい（ＴＴ１７）。なお、認証日付は、認証確認手段１０４０Ａ，Ｂで得られた両者を表示してもよいし、片方を表示してもよい。また、両者の日付が一致している事を判定するようにしてもよい。

【０４９４】また、ステップＴＴ１７では原文書の作成者、各回の変更者の名前などを出力する様にしてもよい。

【０４９５】以上が本実施形態における認証文書確認システム１１０４の全体的な処理流れである。ここで次に図４８におけるステップＴＴ８の処理、つまり、認証確認手段１０４０及び１０４０#n-1の処理についてより具体的に説明する。

【０４９６】図４９は本実施形態の認証確認システムにおける認証確認手段１０４０Ａの処理を示す流れ図である。

【０４９７】同図は、認証確認手段１０４０及び１０４０#n-1の処理の双方を示しているが、ここでは認証確認手段１０４０の処理の場合を例にとって説明する。

【０４９８】まず、認証確認手段１０４０Ａにn回目の認証付き変更電子文書１００８Ｂから認証データの部分が入力される。この認証データ１４０１Ａは、n回目の認証付き変更電子文書１００８Ｂである事を分かる様にした見出し１４０１Ａ－Ｈと、暗号データ１４０１Ａ－Ｄとに分離される（Ｔ８０１、図４６）。なお、n-1…1回目変更の場合にあっては、後述するステップＴ８１１及びＴ８１２にて出力される以前の認証データ及び見出しが上記各データとして用いられる。

【０４９９】このうち、暗号データ１４０１Ａ－Ｄは外部認証機関１０９９の公開鍵１４０２Ａを用いた復号化手段１４０３Ａにより復号され、変更者結合認証データ１４０４Ａ－Ｄが出力される（Ｔ８０２、図４６）。このとき、変更者結合認証データ１４０４Ａ－Ｄと見出し１４０１Ａ－Ｈとは関係付けられ、認証データ１４０４Ａとなる（Ｔ８０３、図４６）。

【０５００】次に、変更者結合認証データ１４０４Ａ－Ｄにある外部認証データ１４０４Ａ－Ｄ２から少なくとも日付データと認証実行ＩＤが取り出され、日付認証手段１０４１に与えられる（Ｔ８０４、図４６）。

【０５０１】一方、変更者結合認証データ１４０４Ａ－Ｄの中の変更者認証データ１４０４Ａ－Ｄ１は分離手段１４０５Ａに与えられ、変更者認証データ１４０６Ａと以前の認証データ１４０７Ａ分離される（Ｔ８０５、図４６）。ここで、以前の認証データ１４０７Ａは原文書の認証からn-1回までの変更文書の認証を含むデータである。以前の認証データ１４０７Ａは認証確認手段１０４０#n-1に与える認証データ１０２７として出力される。

【０５０２】次に、認証確認初回フラグが確認され、初回の場合にはステップＴ８０７が実行され、初回でない場合には、ステップＴ８１０に移動する（Ｔ８０６）。

【０５０３】ステップＴ８０７が実行される場合には、復号化手段１４０９Ａにより、変更者認証データ１４０６Ａが変更者のn回目の公開鍵１４０８Ａで復号化されn回目の特徴データ１４１０Ａが生成される（Ｔ８０７、図４６）。

【０５０４】一方、最終回（ｎ回目）変更にあっては変更電子文書データ１００８Ｂから文書データの部分を受け取り、文書データの特徴が特徴抽出手段１４１１Ａにより抽出され、特徴データ１４１２Ａが出力される（Ｔ８０８、図４６）。なお、n-1 … 1回目変更にあっては認証データ１０２７，１０２７#n-1，…１０２７#2から特徴データが抽出される。

【０５０５】次に、復号化された特徴データ１４１０Ａと認証確認の為に特徴抽出された特徴データ１４１２Ａとが照合手段１４１３Ａにより照合され、その結果が同一性判定手段１０４２に出力される（Ｔ８０９）。同一性判定手段１０４２にて照合結果が一致と判定された場合には、変更電子文書１００８と変更電子文書１００８Ｂとが一致していると証明される。

【０５０６】さらに、認証確認手段１０４０Ａからは、以前の認証データ１４０７Ａが認証データ１０２７として出力され（Ｔ８１１）、今回の変更に関する見出し１４０４Ａ－Ｈが出力される（Ｔ８１２）。これらは、n-1 … 1回目変更の認証に用いられることになる。

【０５０７】次に認証確認手段１０４０のうち、認証確認手段１０４０Ｂ部分の処理を説明する。

【０５０８】図５０は本実施形態の認証確認システムにおける認証確認手段１０４０Ｂの処理を示す流れ図である。

【０５０９】同図は、認証確認手段１０４０及び１０４０#n-1の処理の双方を示しているが、ここでは認証確認手段１０４０の処理の場合を例にとって説明する。

【０５１０】まず、n回目の認証付き変更箇所１００７Ｂから認証データの部分が認証確認手段１０４０Ｂに入力される。この入力された認証データ１４０１Ｂは、n回目の認証付き変更箇所１００７Ｂである事を分かる様にした見出し１４０１Ｂ－Ｈと暗号データ１４０１Ｂ－Ｄとに分離される（Ｔ８２１、図４６）。

【０５１１】次に、暗号データ１４０１Ｂ－Ｄは、復号化手段１４０３Ｂに与えられ、外部認証機関１０９９の公開鍵１４０２Ｂが用いられて復号され、変更者認証データ１４０４Ｂ－Ｄが生成される（Ｔ８２２、図４６）。ここで公開鍵１４０２Ｂは公開鍵１４０２Ａと同じ内容のものである。

【０５１２】また、変更者認証データ１４０４Ｂ－Ｄと見出し１４０４Ｂ－Ｈとが関係付けられ、認証データ１４０４Ｂとされる（Ｔ８２３、図４６）。

【０５１３】変更者認証データ１４０４Ｂ－Ｄにある外部認証データ１４０４Ｂ－Ｄ２から少なくとも外部認証機関１０９９の日付データと認証実行ＩＤとが取り出され、日付認証手段１０４１に与えられる（Ｔ８２４、図４６）。

【０５１４】一方、変更者認証データ１４０４Ｂ－Ｄの中の変更者認証データ１４０４Ｂ－Ｄ１は、復号化手段１４０９Ｂに与えられる。復号化手段１４０９Ｂにおいては、n回目の変更者の公開鍵１４０８Ｂが使用されて、変更者認証データ１４０４Ｂ－Ｄ１が復号化されてn回目の変更箇所の特徴データ１４０１Ｂが取り出される（Ｔ８２７、図４６）。ここで公開鍵１４０８Ｂは公開鍵１４０８Ａと同じ内容のものである。

【０５１５】一方、最終回（ｎ回目）変更にあっては変更箇所データ１００７Ｂから変更箇所データの部分を受け取り、変更箇所データの特徴が特徴抽出手段１４１１Ｂにより抽出され、特徴データ１４１２Ｂが出力される（Ｔ８２８、図４６）。なお、n-1 … 1回目変更にあっては変更箇所データ１００７，１００７#n-1，…１００７#2から特徴データが抽出される。

【０５１６】次に、復号化された特徴データ１４１０Ｂと認証確認の為に特徴抽出された特徴データ１４１２Ｂとが照合手段１４１３Ｂにより照合され、その結果が同一性判定手段１０４２に出力される（Ｔ８２９）。同一性判定手段１０４２にて照合結果が一致と判定された場合には、変更箇所１００７と変更箇所１００７Ｂとが一致していると証明される。なお、より具体的には、認証確認手段１０４０Ａ，Ｂにおける両方の照合手段の結果が両方とも同一の判定である時にn-1回目からn回目の文書変更での文書改竄が無い事が証明されるものである。

【０５１７】さらに、認証確認手段１０４０Ｂからは、今回の変更に関する見出し１４０４Ｂ－Ｈが出力される（Ｔ８３２）。

【０５１８】以上は、主に認証確認手段１０４０による認証確認処理（図４８：ステップＴ８）を説明した。しかし、認証確認手段１０４０#n-1及び１０４３による認証確認処理ではこれと多少異なる部分があるので、その部分について図４７、図４８及び図４９を用いて説明する。

【０５１９】まずは、認証確認手段１０４０#n-1による処理について説明する。

【０５２０】認証確認手段１０４０から出力されたn-1回の認証データ１０２７が、図４７における認証データ１４０１Ａとして認証確認手段１０４０#n-1の認証確認手段１０４０Ａに与えられる。同一性判定手段１０４２#n-1に与えられる比較照合結果がただ一つである点を除けば、以下の処理は、認証確認手段１０４０の場合と同様である。なお、図４７における認証データ１４０７Ａは、認証データ１０２７として次の認証確認手段１０４３に与えられる。

【０５２１】また、認証確認手段１０４３では、認証確認手段１０４０#n-1と同様な処理が繰り返され、n-2回目から1回目までの認証確認が行われる。

【０５２２】上述したように、本発明の実施の形態に係る変更電子文書の改竄防止システム及び方法は、原文及び変更#1から変更#nまでの暗号化特徴データの付加と、原文作成者及び変更者#1から#nまでの本人認証及び外部認証機関の認証とがなされた変更電子文書から、nから1

に向かって順次外部認証機関の認証データを取り出し、また付加されている文書データの特徴データ及び変更箇所の特徴データと確認対象の電子文書本体からの特徴データ及び変更箇所の特徴データとを文書変更者#nから#1までの公開鍵を用いて照合するようにしたので、変更毎の外部認証機関の認証日付には、まさしく変更者#1から#nが文書変更を行なっていた事を証明することができる。

【０５２３】なお、電子文書本体の改竄を行なうと、電子文書１００８Ｂから抽出される特徴データ１４１１Ａが変化する事により、一方、特徴データ１４１０Ａは外部認証機関１０９９によって改竄を防止される事によって、変更者本人であっても外部認証後には文書改竄が不可能になる。

【０５２４】また、変更者#nが電子文書１００８Ｂの差し替えを行うと、外部認証機関１０９９が外部認証手段１０３０Ａ及び外部認証手段１０３０Ｂにより付加した認証実行ＩＤデータが変更若しくは消失していることが日付認証１０４１で発見される。したがって、当該差し替えは不可能である。また、原文１００２Ｂの認証は認証データ１０２７#1を使用するので、原文１００２Ｂ自体の改竄、差し替えも不可能である。

【０５２５】このように変更履歴付電子文書１０１１Ｂは変更者自身のみならず、外部認証機関、その他何人足りとも改竄をする事はできない。

【０５２６】これにより裁判の場で変更文書の原文から変更履歴全ての段階に於いて文書の正当性が証明でき、製造記録や検査記録等の同じ利害関係を持った複数人の変更記録に対しても証拠書類の電子化が可能となる。

【０５２７】また、外部認証機関の認証は特徴データに対して行なわれるので、外部に対して秘密を保持する事が必要な文書に対してもネットワーク１１００として公衆回線を使用しても安全である。

【０５２８】さらに、外部認証機関が認証した原文書、変更箇所、最終文書を結合する事により文書を保存する時の扱いが楽になる。

【０５２９】また、変更文書の各回の変更の認証確認が最終文書から順次溯って復元を行なう必要が無いので、認証の確認が高速で行なえる。

【０５３０】（第１６の実施の形態）本実施形態では、第１４の実施形態の変形例である変更文書の認証システムについて説明する。より正確には、図３９における変更者#nの変更及び認証手段１００６に関する変形例である。

【０５３１】図５１は本発明の第１６の実施形態の文書変更を含んだ電子文書の改竄防止システムにおける変更及び認証手段の機能構成及び処理流れを示す図であり、図４０と同一部分には同一の符号を付して説明を省略する。

【０５３２】図５１に示す文書変更を含んだ電子文書の改竄防止システムは、変更者#nの変更及び認証手段１００６において、図４０の変更者認証手段１０２５Ａに代えて特徴抽出手段１０３３及び変更者認証手段１０３４が設けられる他、第１４の実施形態と同様に構成されている。

【０５３３】ここで、特徴抽出手段１０３３は、変更文書１０２２の特徴を抽出する手段である。また、変更者認証手段１０３４は、結合手段１０２８から出力される結合データを変更者の暗号鍵で暗号化して認証し、認証データ１０２９を出力する手段である。なお、変更者認証手段１０３４は、図４０の変更者認証手段１０２５Ａと類似するものであって、特徴データ１０２５Ａ－２の代わりに、結合手段１０２８により出力される結合データを特徴抽出することなく暗号化するものである。

【０５３４】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について説明する。

【０５３５】まず、変更及び認証手段１００６に与えられたn-1回目の認証付き変更電子文書１００４から、n回目変更変更電子文書１０２２及び認証データ１０２７が得られるところまでは第１４の実施形態と同様である。

【０５３６】次に、n回目変更電子文書１０２２は特徴抽出手段１０３３に入力される。この特徴抽出手段１０３３により生成された特徴データは結合手段１０２８によって、認証データ１０２７と結合される。この結合手段１０２８によって結合されたデータは、変更者認証手段１０３４に与えられ暗号化されて、n回目変更文書の変更者結合認証データ１０２９が作成される。

【０５３７】以下、第１４の実施形態と同様な処理が行われる。

【０５３８】上述したように、本発明の実施の形態に係る変更電子文書の改竄防止システム及び方法は、第１４の実施形態と同様な構成を有する他、特徴抽出手段１０３３及び変更者認証手段１０３４を設けたので、第１４の実施形態と同様な効果が得られる他、変更文書本体の改竄を行なうと改竄後の文書から抽出されるべき特徴データが変化し、先に認証用に抽出された特徴データ１０３３と異なるものになる事によって、変更文書本体の改竄の事実を検出することができる。

【０５３９】また、一方先に認証用に抽出された特徴データ１０３３は外部認証機関の認証データ１０３０Ａ－Ａとともに認証機関の秘密鍵１０３０Ａ－２で暗号化されているので、認証付き変更電子文書１００８に付されている認証データ１０３２Ａの改竄は不可能である。従って、たとえ本人であっても外部認証後には文書改竄が不可能になる。

【０５４０】(第１７の実施の形態)本実施形態では、第１５の実施形態の変形例である変更文書の認証確認システムについて説明する。より正確には、図４５の認証確認手段１０４０及び１０４０#n-1に関する変形例であ

る。

【０５４１】図５２は本発明の第１７の実施形態の文書変更を含んだ電子文書の改竄防止システムにおける認証確認手段の機能構成及び処理流れを示す図であり、図４５と同一部分には同一の符号を付して説明を省略する。

【０５４２】図５２に示す文書変更を含んだ電子文書の改竄防止システムは、認証確認手段１０４０、１０４０#n-1及び１０４３において、分離手段１４０５Ａに代えて分離手段１４１４Ａが設けられる他、第１５の実施形態と同様に構成されている。

【０５４３】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について説明する。

【０５４４】まず、認証確認手段１０４０Ａにおいて、変更結合認証データ１４０４Ａが得られるところまでは、第１５の実施形態と同様である。

【０５４５】ここで、変更者結合認証データ１４０４Ａ－Ｄは、復号化手段１４０９Ａに与えられ、n回目の変更者の公開鍵１４０８Ａにより変更者結合認証データ復号される。復号データはさらに分離手段１４１４Ａによって分離され、特徴データ１４１０Ａと認証データ１４０７Ａとなる。

【０５４６】以下、第１５と同様な処理が行われる。

【０５４７】なお、認証確認手段１０４０#n-1及び１０４３においても、同様な処理が行われる。

【０５４８】上述したように、本発明の実施の形態に係る変更電子文書の改竄防止システム及び方法は、第１５の実施形態と同様な構成を有する他、分離手段１４０５Ａに代えて分離手段１４１４Ａを設けたので、第１５の実施形態と同様な効果を得ることができる。

【０５４９】なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。

【０５５０】例えば各実施形態では単に電子文書１とのみ表現するが、この電子文書なるものは電子情報ならば文書に限らず何でもよい。例えば映像データ、音声データ、プログラムソースファイル、プログラム実行ファイル等のバイナリデータをも含む。

【０５５１】さらに、実施形態では主として公開鍵暗号方式の場合を説明しているが、本発明はこれに限られるものではなく、例えば秘密鍵暗号方式を用いてもよい。

【０５５２】また、実施形態に記載した手法は、計算機（コンピュータ）に実行させることができるプログラム（ソフトウエア手段）として、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ等）、半導体メモリ等の記憶媒体に格納し、また通信媒体により伝送して頒布することもできる。なお、媒体側に格納されるプログラムには、計算機に実行させるソフトウエア手段（実行プログラムのみならずテーブルやデータ構造も含む）を計算機内に構成させる設定プログラムをも含むものである。本装置を実現する計算機は、記憶媒体に記録されたプログラムを読み込み、また場合により設定プログラムによりソフトウエア手段を構築し、このソフトウエア手段によって動作が制御されることにより上述した処理を実行する。

【０５５３】

【発明の効果】以上詳記したように本発明によれば、作成者本人自身による改竄をも防止した電子文書が提供できるので、重要文書や公的文書など従来は紙でなければ運用出来なかったものに対しても電子文書での運用が可能になり真の意味での電子化を実現させることを可能とした電子文書の改竄防止システム及び方法を提供することができる。

【０５５４】このように改竄を防止した電子文書化により、遠隔地でも重要文書を瞬時のうちに送達する事ができるようになる。また、電子契約書の実現により、契約書にサインを行う場合でも離れた場所で瞬時のうちにサインを交わす事ができる。電子文書化により文書の保管場所を取らなくなる。電子文書化により文書の検索が可能になる等、その効果は極めて大である。

【０５５５】また、本発明によれば、電子文書の特徴データからは電子文書の内容を伺い知る事ができないので、企業の秘密文書について外部認証機関の認証を行う事ができ、機密漏洩の危険から免れる事ができる電子文書の改竄防止システム及び方法を提供することができる。

【０５５６】さらに、本発明によれば、電子文書の特徴データを高速で作成でき、また圧縮率も高いので、特徴データ抽出時間とデータの伝送時間の短縮ができる電子文書の改竄防止システム及び方法を提供することができる。

【０５５７】さらにまた、本発明によれば、指紋データを使用し暗号鍵および秘密鍵を暗号化する事により本人認証データを盗まれる事が有っても他人にはそのデータを利用できないので、本人認証データの信頼性を非常に高くすることができる電子文書の改竄防止システム及び方法を提供することができる。

【０５５８】また、本発明によれば、複数人が複数時期に渡って一つの電子文書を作成する場合でも、変更文書を関係者全員で再承認する必要をなくしかつ文書改竄を防止して、紙文書の証拠能力以上の証拠能力を有する電子文書を作成可能とした電子文書の改竄防止システム及び方法を提供することができる。

【０５５９】このように作製者自身による改竄をも防止した変更電子文書が提供できるので、重要文書や公的文書など従来は紙でなければ運用できなかったものに対しても電子文書上での部分変更の運用が可能となる。また、各種設計資料や、設計図面、製作資料や製作図、試験資料や試験データ、試験結果、検査資料や検査結果など、企業の中で使用される文書で社外に開示をしたくな

い資料について、それらのドキュメントの内容と製作時期、変更内容と変更時期が証明されるので、製品事故などが発生した時の非常に有力な裁判資料として使用できる。とくに、設計工程、製造工程、検査工程の中等で、１枚の紙に複数の時期にわたって内容が追記されていくチェックシート等が裁判の場で正当性を証明できる資料としての電子化を実現する。

【図面の簡単な説明】

【図１】本発明の各実施形態における電子文書の作成システム及び方法の全体的な構成を示す図。

【図２】本発明の第１の実施の形態に係る電子文書の改竄防止システムに適用される文書認証システムのハードウエア構成例を示すブロック図。

【図３】同実施形態の電子文書の改竄防止システムに適用される外部認証システムのハードウエア構成例を示すブロック図。

【図４】同実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図５】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図６】本発明の第２の実施の形態に係る電子文書の改竄防止システムに適用される認証文書確認システムのハードウエア構成例を示すブロック図。

【図７】同実施形態の電子文書の改竄防止システムに適用される認証文書確認システムの機能構成及び処理流れの一例を示す図。

【図８】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図９】本発明の第３の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図１０】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図１１】本発明の第４の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図１２】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図１３】本発明の第５の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図１４】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図１５】本発明の第６の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図１６】本発明の第７の実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図１７】同実施形態の電子文書の改竄防止システムの電子印鑑生成処理を示す流れ図。

【図１８】同実施形態の電子文書の改竄防止システムの電子印鑑照合処理を示す流れ図。

【図１９】同実施形態の電子文書の改竄防止システムの文書見出し編集処理を示す流れ図。

【図２０】本発明の第８の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図。

【図２１】同実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図２２】同実施形態の電子文書の改竄防止システムの特徴データ抽出の処理の一例を示す流れ図。

【図２３】本発明の第９の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図。

【図２４】本発明の第１０の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図。

【図２５】同実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図２６】同実施形態の電子文書の改竄防止システムの特徴データ抽出の処理の一例を示す流れ図。

【図２７】本発明の第１１の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図２８】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図２９】本発明の第１２の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図３０】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図３１】本発明の第１３の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図３２】指紋データの一例を示す図。

【図３３】指紋データから矩形領域に切り出したデータの一例を示す図。

【図３４】マッチングさせるパターンの例の一部分を示した図。

【図３５】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図３６】本発明の第１４～第１７の実施形態における文書変更を含んだ電子文書の改竄防止システム及び方法の全体的な構成を示す図。

【図３７】本発明の第１４の実施形態に係る文書変更を含んだ電子文書の改竄防止システムに適用される文書変更認証システムのハードウェア構成例を示すブロック図。

【図３８】同実施形態の文書変更を含んだ電子文書の改竄防止システムに適用される外部認証システムのハードウェア構成例を示すブロック図。

【図３９】同実施形態の文書変更を含んだ電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図４０】同実施形態の文書変更を含んだ電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図４１】変更者#nの変更及び認証手段における変更者認証手段の構成を示す図。

【図４２】外部認証システムにおける外部認証手段の構成を示す図。

【図４３】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図４４】本発明の第１５の実施の形態に係る変更電子文書の改竄防止システムに適用される認証文書確認システムのハードウェア構成例を示すブロック図。

【図４５】同実施形態の変更電子文書の改竄防止システムに適用される認証文書確認システムの機能構成ならびに処理流れの一例を示す図。

【図４６】認証確認手段１０４０の詳細構成を示す図。

【図４７】認証確認手段１０４０#n-1の詳細構成を示す図。

【図４８】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図４９】同実施形態の認証確認システムにおける認証確認手段１０４０Ａの処理を示す流れ図。

【図５０】同実施形態の認証確認システムにおける認証確認手段１０４０Ｂの処理を示す流れ図。

【図５１】本発明の第１６の実施形態の文書変更を含んだ電子文書の改竄防止システムにおける変更及び認証手段の機能構成及び処理流れを示す図。

【図５２】本発明の第１７の実施形態の文書変更を含んだ電子文書の改竄防止システムにおける認証確認手段の機能構成及び処理流れを示す図。

【図５３】電子文書に署名してその同一性を判定する従来の方法を示す図。

【符号の説明】

１…電子文書
２…特徴抽出手段
２Ｔ…セパレータテーブル
２Ｗ…単語配列
３…見出し付き特徴データ
３Ｈ…見出し
３Ｄ…特徴データ
４…秘密鍵
５…暗号化手段
６…見出し付き暗号データ
６Ｈ…見出し
６Ｄ…暗号データ
７…見出し付き認証データ
７Ｈ…見出し
７Ｄ…暗号データ
７Ａ…外部認証データ
８…秘密鍵
９…暗号化手段
１０…合成データ
１０Ｈ…見出し
１０Ｄ…暗号データ
１１…合成データ
１１Ｈ…見出し
１１Ｄ…暗号データ
１２…認証付電子文書
１３…公開鍵
１４…復号化手段
１５…見出し付き認証データ
１５Ｈ…見出し
１５Ｄ…暗号データ
１５Ａ…外部認証データ
１５Ａ－Ｄ…日付認証
１６…公開鍵
１７…復号化手段
１８…見出し付き特徴データ
１８Ｈ…見出し
１８Ｄ…特徴データ
１９…電子文書
２０…特徴抽出手段
２１…特徴データ
２２…照合手段
２２－Ｊ…同一性判定
２３…見出し付き認証データ
２３Ｈ…見出し
２３Ｄ…暗号データ
２３Ａ…外部認証データ
２４…秘密鍵
２５…暗号化手段
２６…見出し付き暗号データ
２６Ｈ…見出し
２６Ｄ…暗号データ
２７…見出し付き暗号データ
２７Ｈ…見出し
２７Ｄ…暗号データ
２８…認証付電子文書
２９…公開鍵
３０…復号化手段
３１…見出し付き認証データ
３１Ｈ…見出し
３１Ｄ…暗号データ
３１Ａ…外部認証データ
３１Ａ－Ｄ…日付認証
３２…見出し付き認証データ
３２Ｈ…見出し
３２Ｄ…暗号データ
３２Ａ…外部認証データ
３３…秘密鍵

３４…暗号化手段
３５…見出し付き暗号データ
３５Ｈ…見出し
３５Ｄ…暗号データ
３６…見出し付き認証データ
３６Ｈ…見出し
３６Ｄ…暗号データ
３６Ａ…外部認証データ
３７…秘密鍵
３８…暗号化手段
３９…見出し付き暗号データ
３９Ｈ…見出し
３９Ｄ…暗号データ
４０…見出し付き暗号データ
４０Ｈ…見出し
４０Ｄ…暗号データ
４１…認証付電子文書
４２…公開鍵
４３…復号化手段
４４…見出し付き認証データ
４４Ｈ…見出し
４４Ｄ…暗号データ
４４Ａ…外部認証データ
４４Ａ－Ｄ…日付認証
４５…公開鍵
４６…復号化手段
４７…見出し付き認証データ
４７Ｈ…見出し
４７Ｄ…暗号データ
４７Ａ…外部認証データ
４７Ａ－Ｄ…日付認証
４８…公開鍵
４９…復号化手段
５０…見出し付き特徴データ
５０Ｈ…見出し
５０Ｄ…特徴データ
５１…特徴抽出手段
５２…特徴データ
５３…照合手段
５３－Ｊ…同一性判定
５４…印影
５５…特徴抽出手段
５６…特徴データ
５８…暗号化手段
５９…暗号化印影
６０…電子印鑑
６１…日付署名印影情報
６２…整形手段
６３…文書表示手段
６４…指紋読取り機

６５…指紋
６６…特徴抽出手段
６６Ｓ…切り出し手段
６６ＳＤ…データ
６６Ｍ…マッチング手段
６６Ｐ…パターン
６６Ｄ…１桁分データ
６７…特徴データ
６８…パスワード
６９…氏名・ＩＤ
７０…暗号鍵生成手段
７１…暗号鍵
７２…乱数発生器
７３…秘密鍵公開鍵生成手段
７４…秘密鍵
７５…公開鍵
７６…暗号化手段
７７…暗号化秘密鍵
７８…本人認証データ
７８Ｆ…指紋
７８Ｓ…暗号化秘密鍵
７８Ｋ…暗号化暗号鍵
７８Ｐ…パスワード
７８Ｎ…氏名・ＩＤ
７９…表示手段
８０…照合手段
８１…照合手段
８２…判定ロジック
８３…復号手段
８４…暗号鍵
８５…照合手段
８６…復号手段
８７…指紋データ抽出手段
８７Ｆ…原指紋データ
８７Ａ…境界抽出手段
８７Ｅ…エンボス手段
８７Ｌ…輪郭抽出手段
８７Ｂ…２値化
９７，９８…記録媒体
９９…外部認証機関
１００…ネットワーク
１０１…文書認証システム
１０２…外部認証システム
１０３…認証文書確認システム
１１０…計算機
１１１…表示装置
１１２…入力装置
１１３…印刷装置
１１４…外部記憶装置
１１５…スキャナ

83

１１６…ＣＰＵバス
１１７…ＣＰＵ
１１８…ＲＯＭ
１１９…ＲＡＭ
１２０，１２１，１２２，１２３，１２４，１２５，１２６，１２７…インターフェース手段
１２８…ハードディスク装置
１２９…通信装置
１３０…プログラム格納部
１３１…データ格納部
１３２…作業領域
１３３…文書認証プログラム
１３４…外部認証プログラム
１３５…認証文書確認プログラム
１００１…変更履歴付電子文書
１００２…原電子文書
１００２Ｂ…認証確認対象の原電子文書
１００３…変更箇所
１００４…変更電子文書
１００５…分離手段
１００６…変更及び認証手段
１００７…変更箇所
１００７Ｂ…n回変更箇所
１００７Ｂ#n-1…n-1回変更箇所
１００８…変更電子文書
１００８Ｂ…認証確認対象の変更電子文書
１００９…結合手段
１０１０…変更箇所
１０１１…変更履歴付電子文書
１０１１Ｂ…認証確認対象の変更履歴付電子文書
１０２０…変更電子文書
１０２１…変更手段
１０２２…変更電子文書
１０２３…差分抽出手段
１０２４…変更箇所
１０２５Ａ，１０２５Ｂ…変更者認証手段
１０２５Ａ－１…特徴抽出手段
１０２５Ａ－２…特徴データ
１０２５Ａ－３…変更者#n秘密鍵
１０２５Ａ－４…暗号化手段
１０２６Ａ，１０２６Ｂ…変更者認証データ
１０２６Ａ－Ｈ…見出し
１０２６Ａ－Ｄ…暗号データ
１０２７…認証データ
１０２７#n-1…認証データ
１０２８…結合手段
１０２９…結合認証データ
１０３０Ａ，１０３０Ｂ…外部認証手段
１０３０Ａ－Ａ…外部認証データ
１０３０Ａ－１…結合手段

84

１０３０Ａ－２…外部秘密鍵
１０３０Ａ－３…暗号化手段
１０３１Ａ，１０３１Ｂ…認証データ
１０３１Ａ－Ｄ…暗号データ
１０３１Ａ－Ｈ…見出し
１０３２Ａ，１０３２Ｂ…認証データ
１０３３…特徴抽出手段
１０３４…変更者認証手段
１０４０…認証確認手段
１０４０Ａ，１０４０Ｂ…認証確認手段
１０４０#n-1…認証確認手段
１０４１…日付認証
１０４１#n-1…日付認証
１０４２…同一性判定
１０４２#n-1…同一性判定
１０４３…認証確認(繰返し)
１０４４…認証確認手段
１０４５…日付認証
１０４６…同一性判定
１０９７，１０９８…記録媒体
１０９９…外部認証機関
１１００…ネットワーク
１１０１…文書認証システム
１１０２…外部認証システム
１１０３…文書変更認証システム
１１０４…認証文書確認システム
１１１０…計算機
１１１１…表示装置
１１１２…入力装置
１１１３…印刷装置
１１１４…外部記憶装置
１１１５…スキャナ
１１１６…ＣＰＵバス
１１１７…ＣＰＵ
１１１８…ＲＯＭ
１１１９…ＲＡＭ
１１２０～１１２７…インターフェイス手段
１１２８…ハードディスク装置
１１２９…通信装置
１１３０…プログラム格納部
１１３１…データ格納部
１１３２…作業領域
１１３３…文書変更認証プログラム
１１３４…外部認証プログラム
１１３５…認証文書確認プログラム
１４０１Ａ…認証データ
１４０１Ａ－Ｄ…暗号データ
１４０１Ａ－Ｈ…見出し
１４０２Ａ…外部認証機関の公開鍵
１４０３Ａ…復号化手段

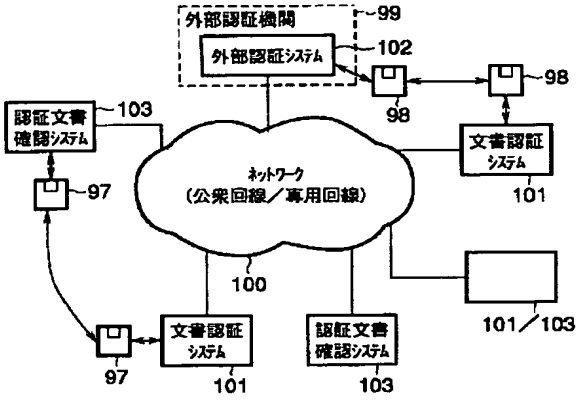
85

１４０４Ａ…変更者結合認証データ
１４０４Ａ－Ｄ…変更者結合認証データ
１４０４Ａ－Ｄ１…変更者認証データ
１４０４Ａ－Ｄ２…外部認証データ
１４０４Ａ－Ｈ…見出し
１４０５Ａ…分離手段
１４０６Ａ…変更者認証データ
１４０７Ａ…以前の認証データ
１４０８Ａ…変更者の公開鍵
１４１０Ａ…特徴データ
１４１１Ａ…特徴抽出手段
１４１２Ａ…特徴データ

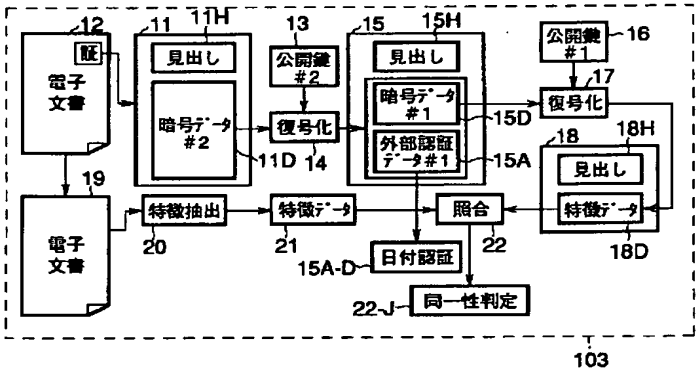
86

１４１３Ａ，１４１３Ｂ…照合手段
１４１４Ａ…分離手段
Ｓ…電子文書データ並び
Ｓ１，Ｓ２，Ｓ３…電子文書データ並び部分
Ｓ＿ｓｕｍ…合計値
Ｓ＿ｓ＿ｓｔｒｅａｍ…合計データ並び
ＩＳ…間隔を置いたデータ並び
ＩＳ１，ＩＳ２，ＩＳ３…間隔を置いたデータ並び部分
ＩＳ＿ｓｕｍ［０］，．．，ＩＳ＿ｓｕｍ［２５５］…間隔を置いたデータの合計値の配列
ＩＳ＿ｓ＿ｓｔｒｅａｍ…間隔を置いた合計データ並び
ｉ，ｊ…カウンタ

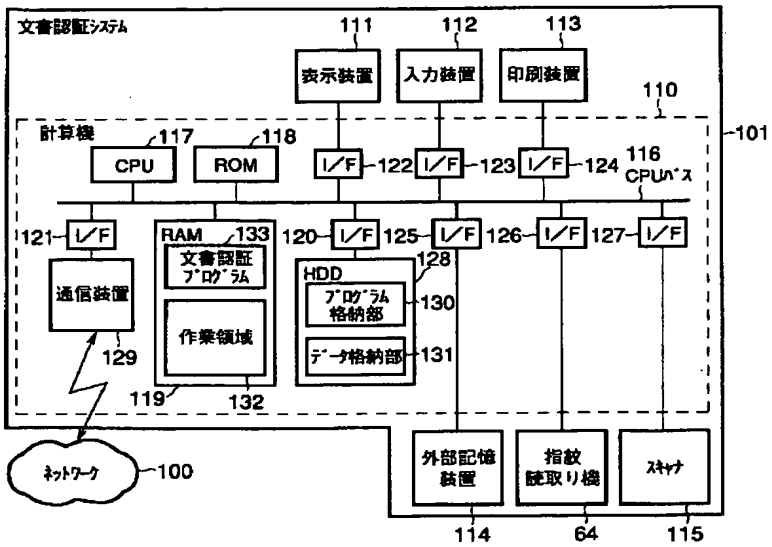
【図１】



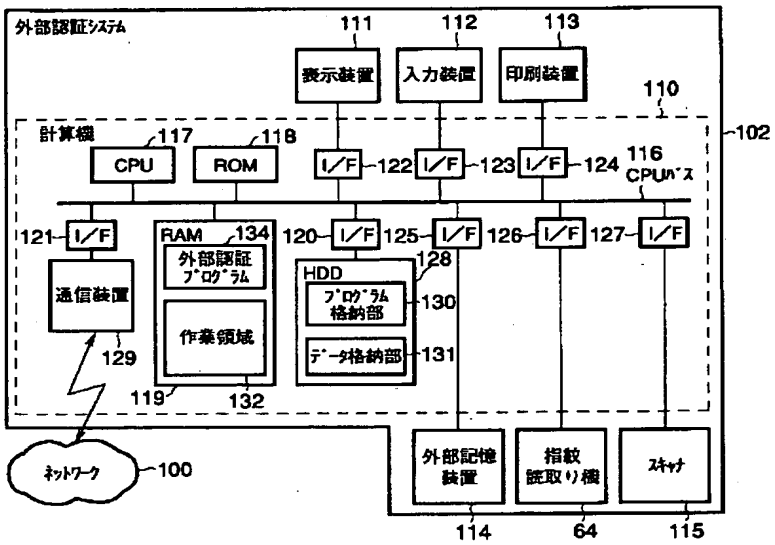
【図７】



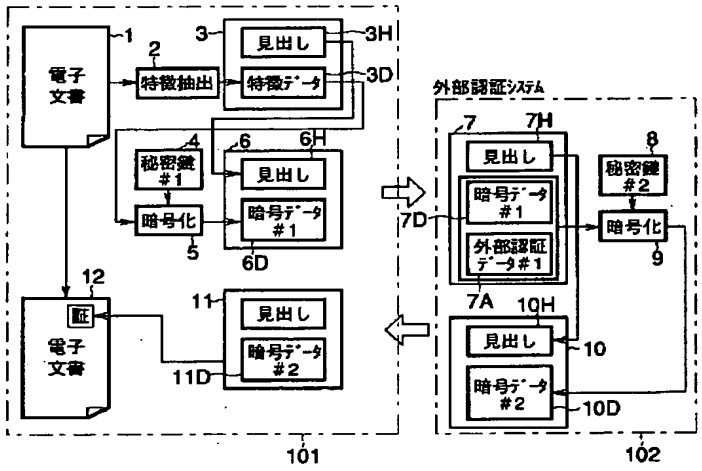
【図２】



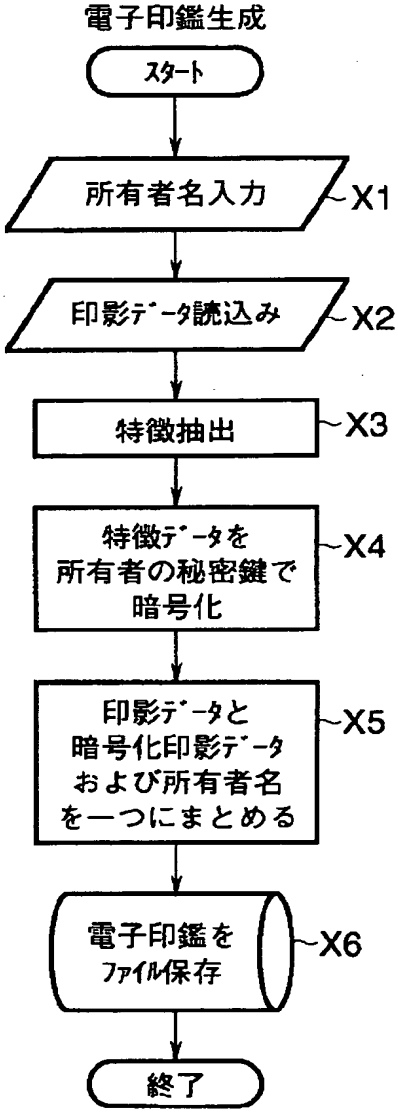
【図３】


外部認証システム
111
112
113
表示装置
入力装置
印刷装置
110
102
計算機
117
118
CPU
ROM
I/F
122
123
124
116
CPUバス
121
RAM
134
120
125
126
127
外部認証プログラム
作業領域
HDD
128
プログラム格納部
130
データ格納部
131
通信装置
129
119
132
ネットワーク
100
外部記憶装置
指紋読取り機
スキャナ
114
64
115

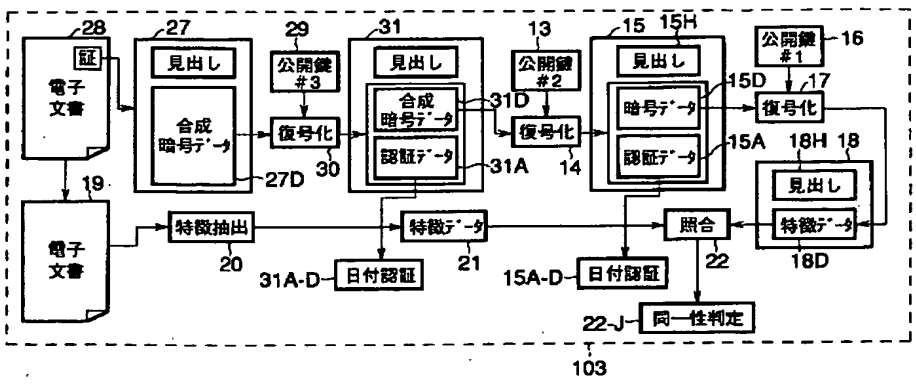
【図４】


電子文書
1
特徴抽出
2
3
見出し
特徴データ
3H
3D
秘密鍵#1
4
暗号化
5
6
6H
暗号データ#1
6D
12
証
11
11D
暗号データ#2
101
外部認証システム
7
7H
外部認証データ#1
7D
秘密鍵#2
8
9
7A
10H
10
10D
102

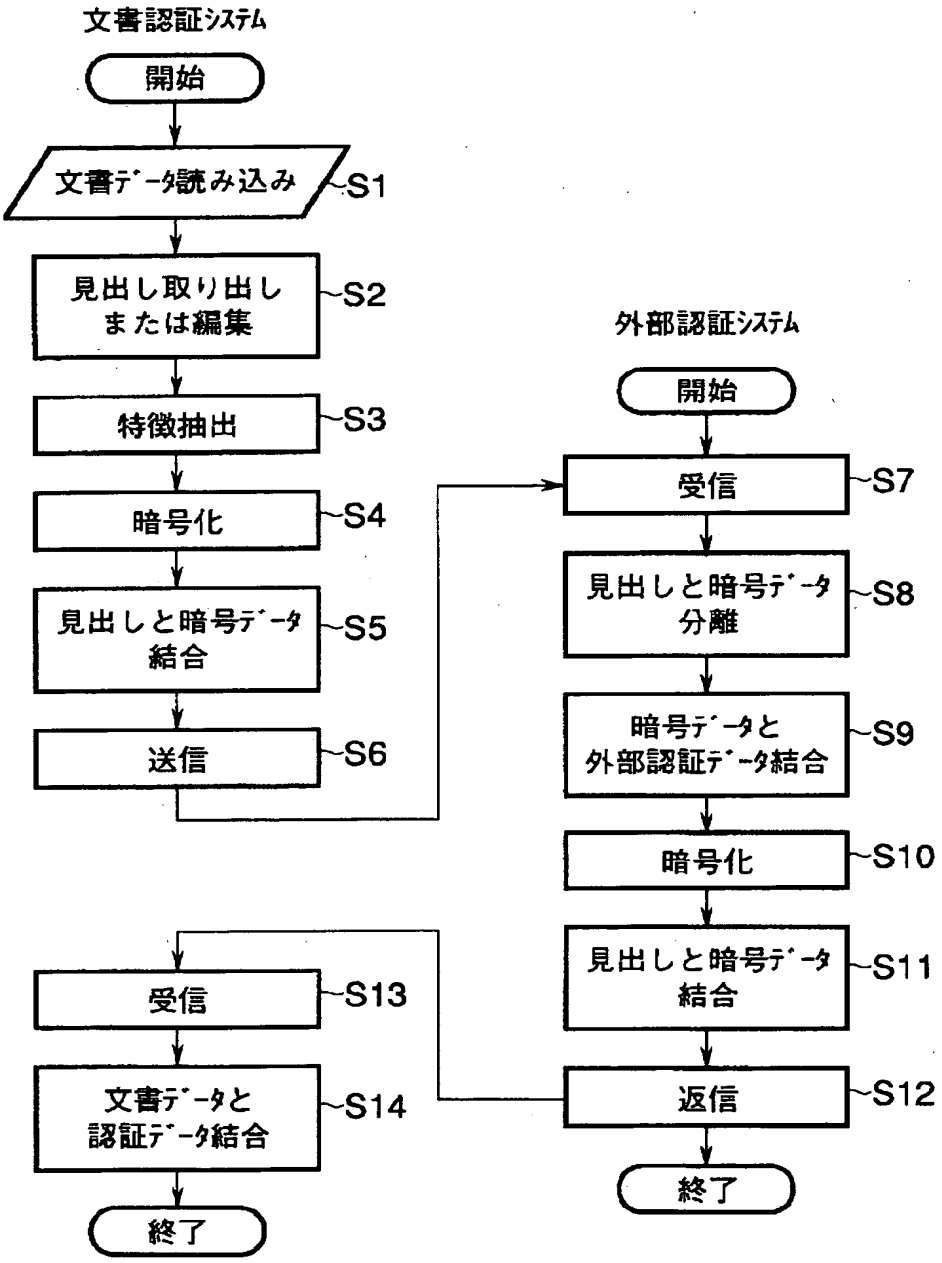
【図１７】


電子印鑑生成
スタート
所有者名入力
X1
印影データ読込み
X2
特徴抽出
X3
特徴データを所有者の秘密鍵で暗号化
X4
印影データと暗号化印影データおよび所有者名を一つにまとめる
X5
電子印鑑をファイル保存
X6
終了

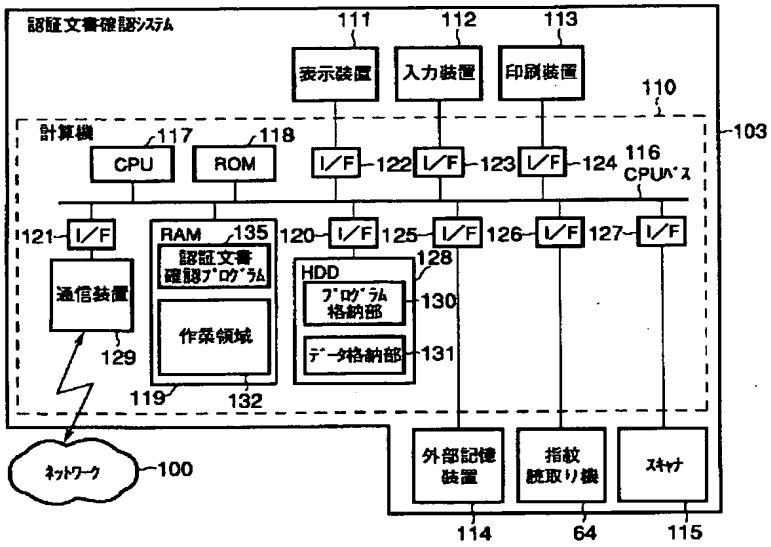
【図１１】


28
証
電子文書
19
27
見出し
合成暗号データ
27D
29
公開鍵#3
復号化
30
31
見出し
合成暗号データ
認証データ
31A
31D
13
公開鍵#2
復号化
14
15
15H
見出し
暗号データ
認証データ
15A
15D
公開鍵#1
16
復号化
17
18H
18
見出し
特徴データ
18D
特徴抽出
20
特徴データ
21
照合
22
31A-D
日付認証
15A-D
日付認証
22-J
同一性判定
103

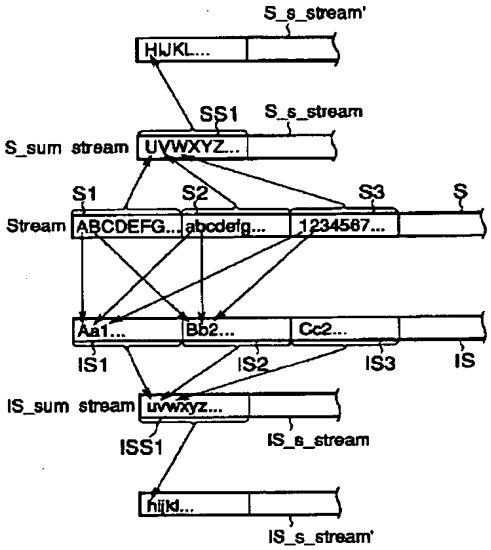
【図５】


文書認証システム
開始
文書データ読み込み
S1
見出し取り出し
または編集
S2
特徴抽出
S3
暗号化
S4
見出しと暗号データ
結合
S5
送信
S6
受信
S13
文書データと
認証データ結合
S14
終了
外部認証システム
開始
受信
S7
見出しと暗号データ
分離
S8
暗号データと
外部認証データ結合
S9
暗号化
S10
見出しと暗号データ
結合
S11
返信
S12
終了

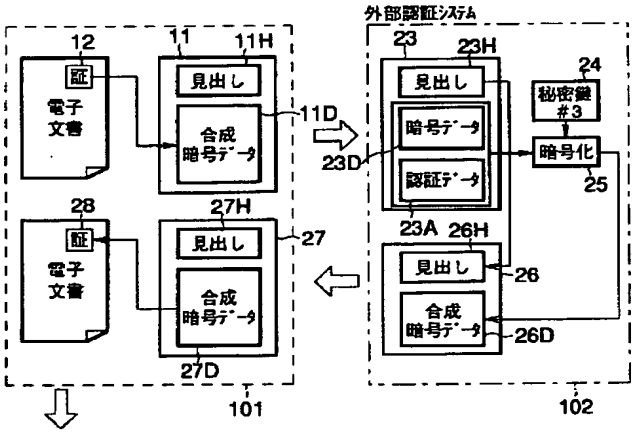
【図６】



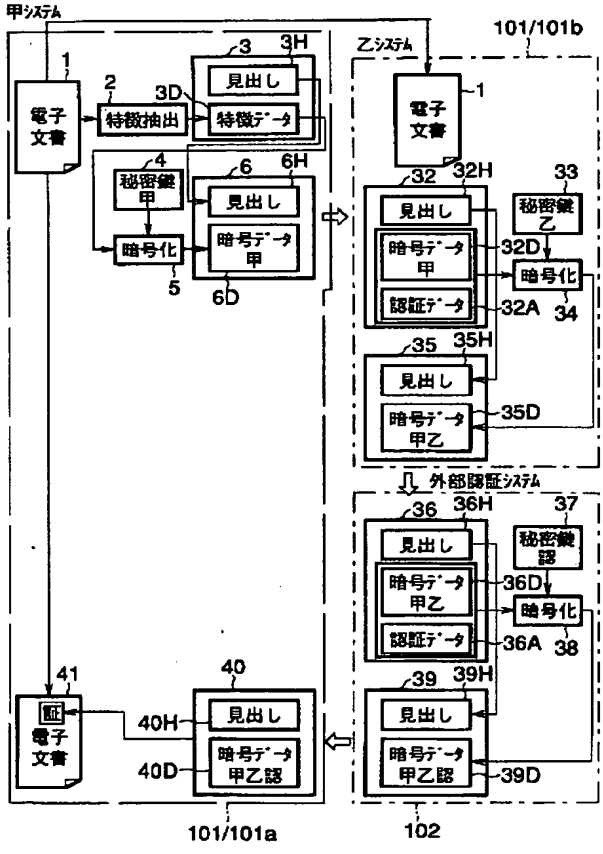
【図２３】



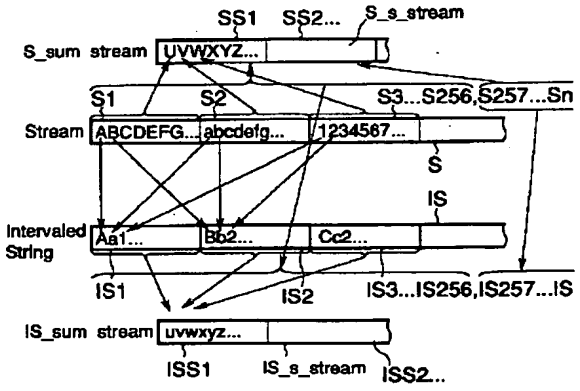
【図９】



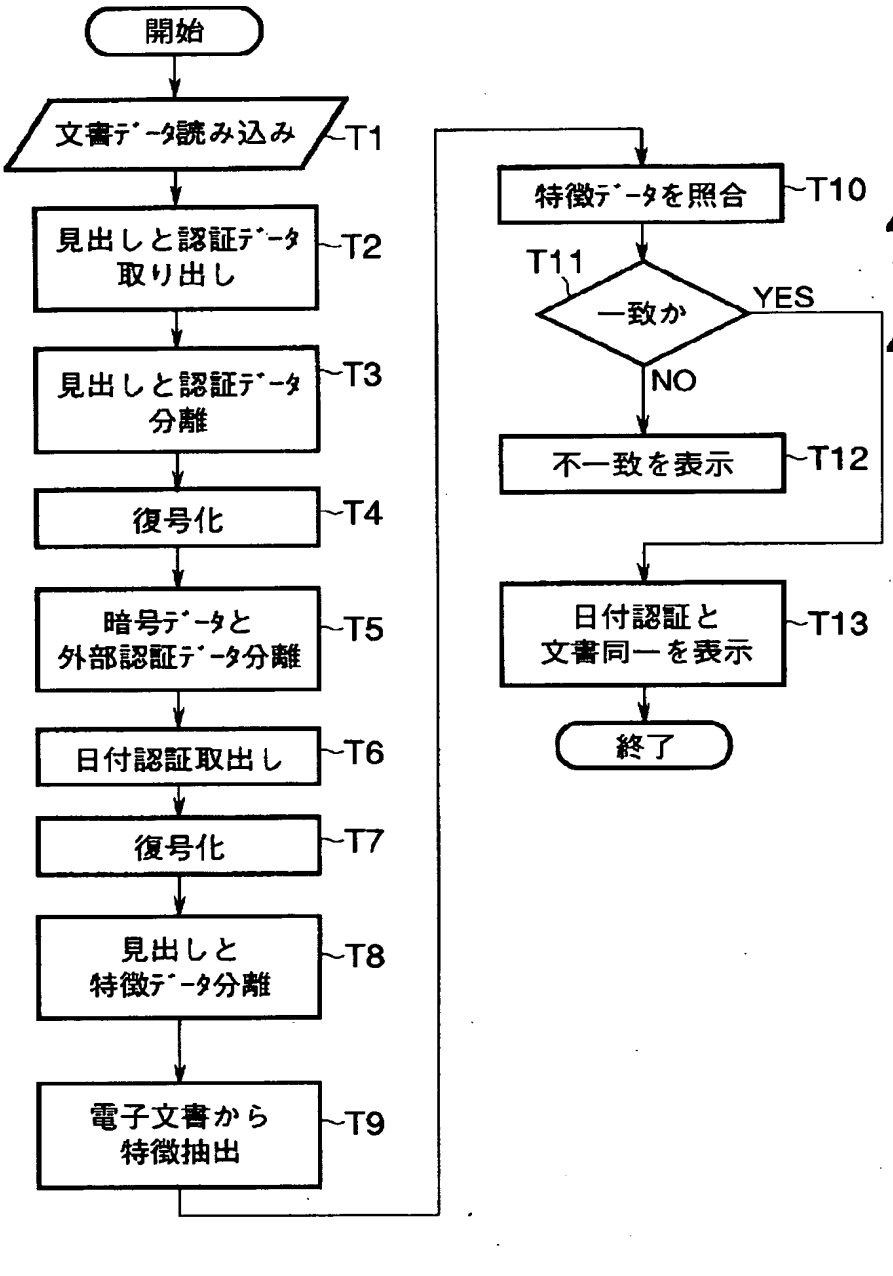
【図１３】



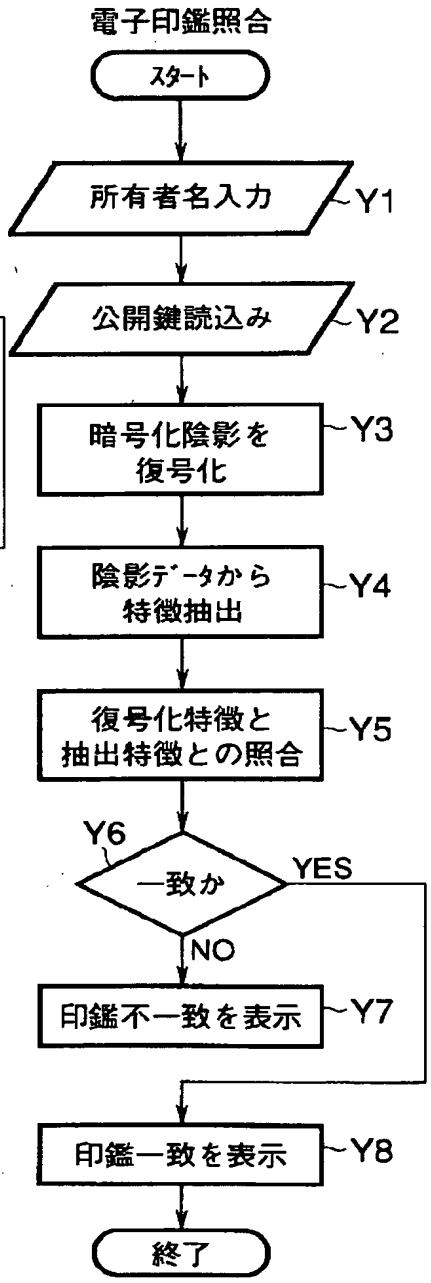
【図２０】



【図８】



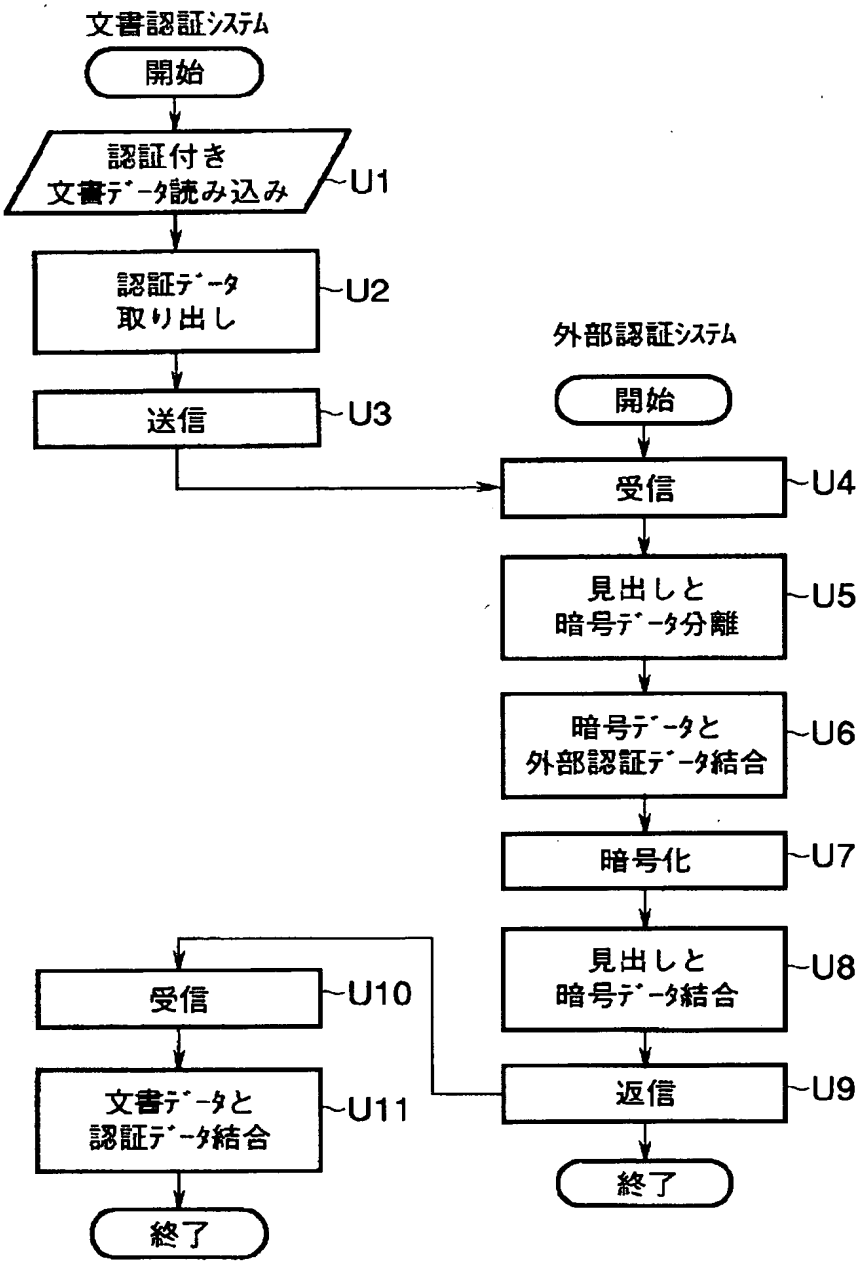
【図１８】



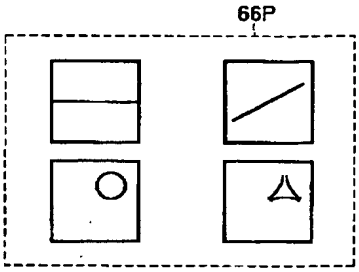
【図３２】

【図３３】

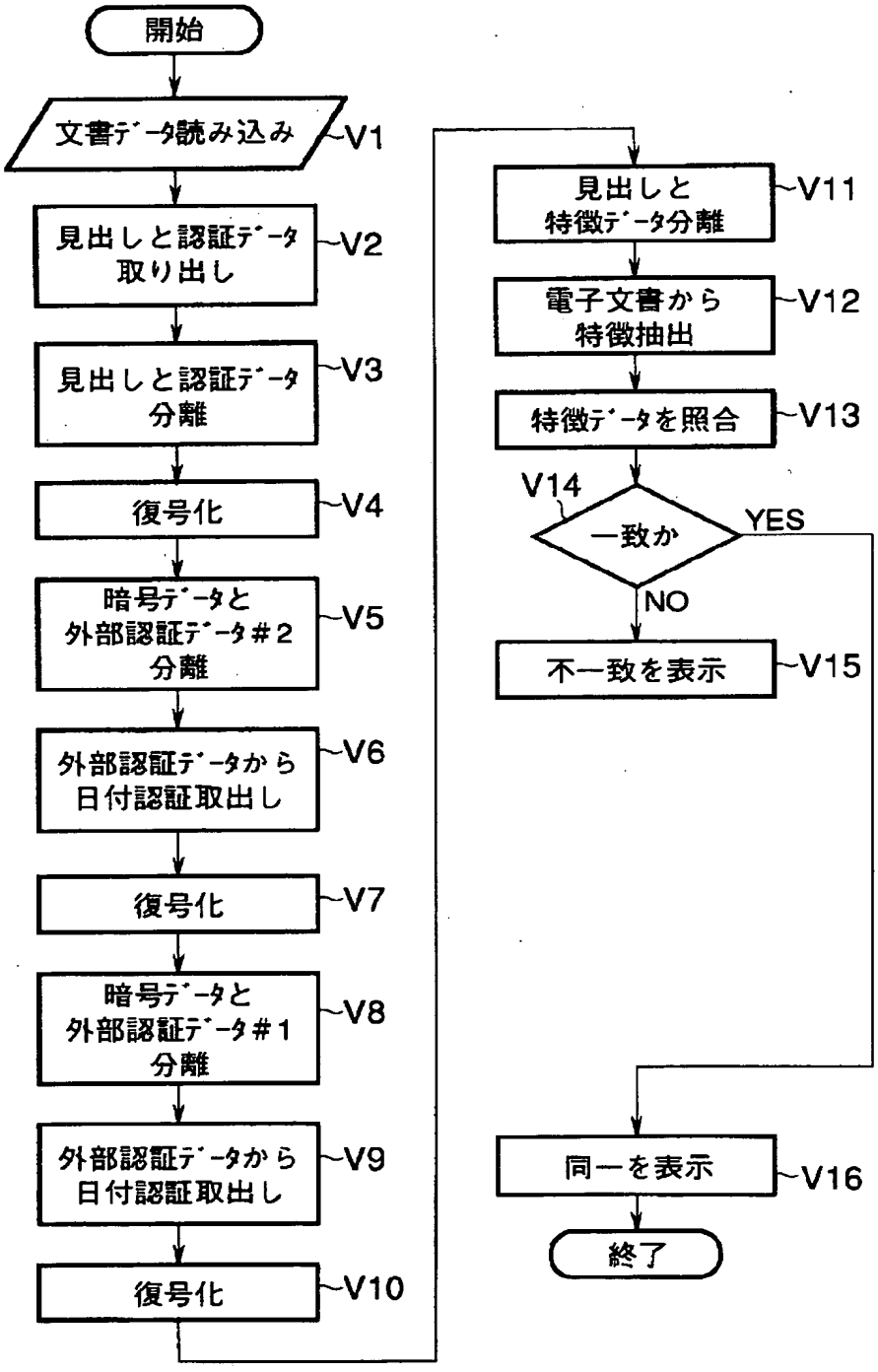
【図１０】


文書認証システム
開始
認証付き
文書データ読み込み
U1
認証データ
取り出し
U2
送信
U3
外部認証システム
開始
受信
U4
見出しと
暗号データ分離
U5
暗号データと
外部認証データ結合
U6
暗号化
U7
見出しと
暗号データ結合
U8
返信
U9
終了
受信
U10
文書データと
認証データ結合
U11
終了

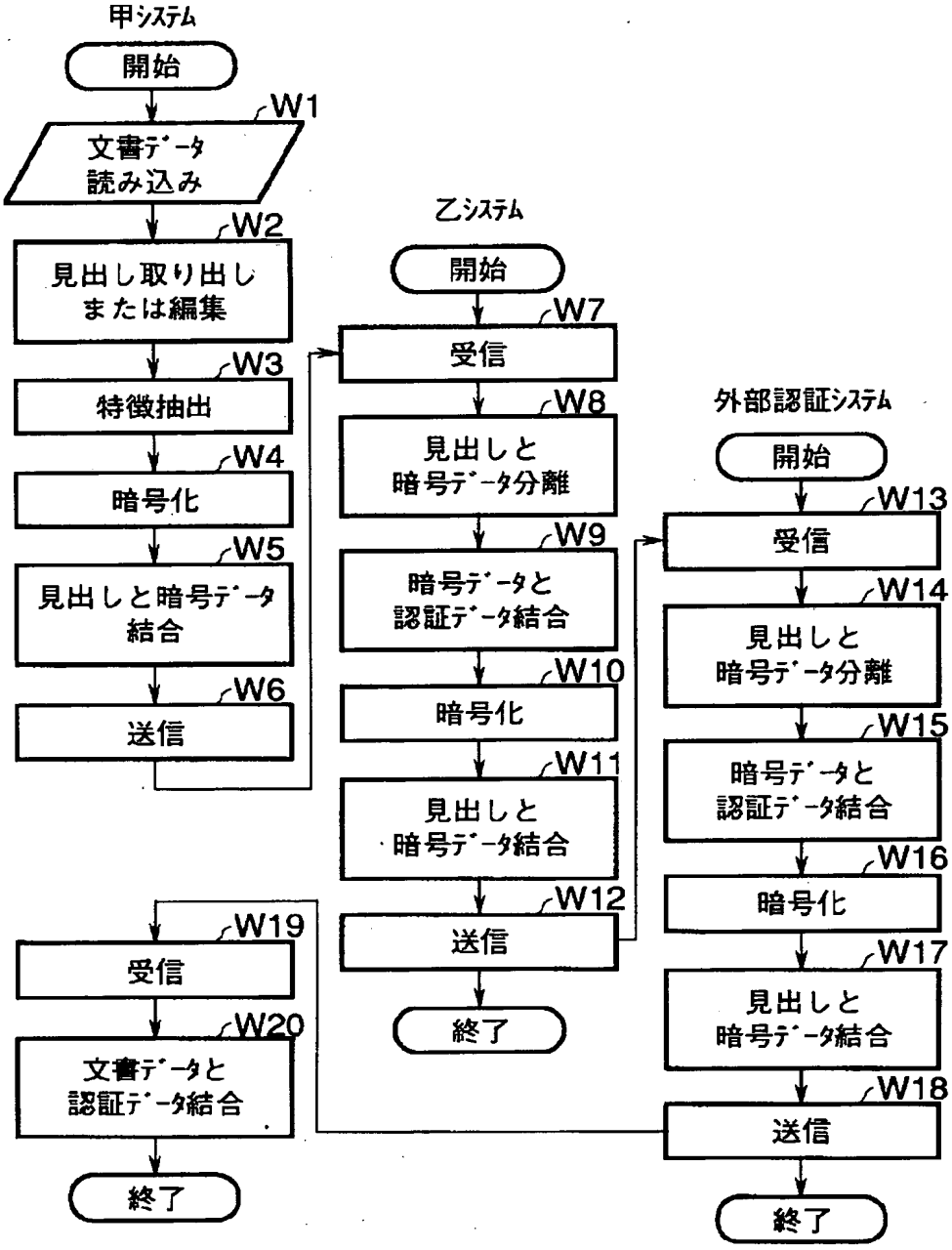
【図３４】


66P

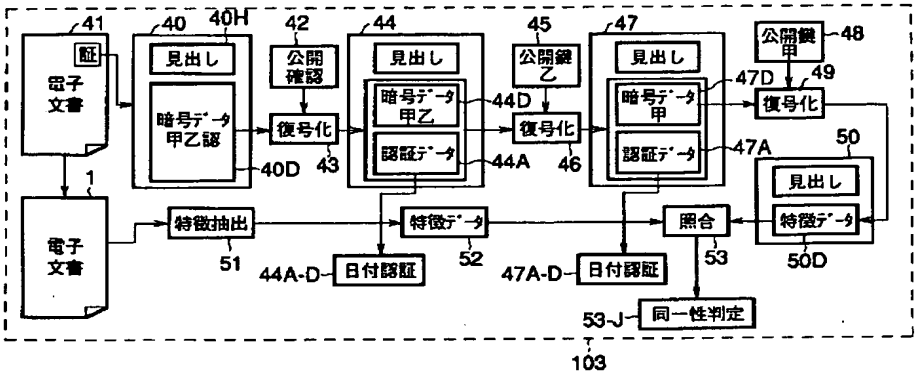
【図１２】


開始
文書ﾃﾞｰﾀ読み込み
V1
見出しと認証ﾃﾞｰﾀ取り出し
V2
見出しと認証ﾃﾞｰﾀ分離
V3
復号化
V4
暗号ﾃﾞｰﾀと外部認証ﾃﾞｰﾀ＃２分離
V5
外部認証ﾃﾞｰﾀから日付認証取出し
V6
復号化
V7
暗号ﾃﾞｰﾀと外部認証ﾃﾞｰﾀ＃１分離
V8
外部認証ﾃﾞｰﾀから日付認証取出し
V9
復号化
V10
見出しと特徴ﾃﾞｰﾀ分離
V11
電子文書から特徴抽出
V12
特徴ﾃﾞｰﾀを照合
V13
V14
一致か
YES
NO
不一致を表示
V15
同一を表示
V16
終了

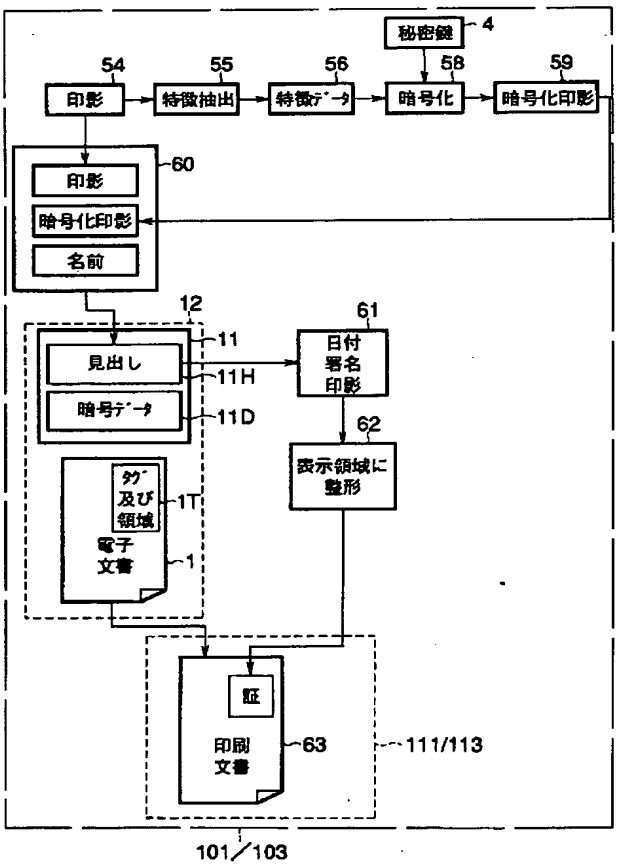
【図１４】


甲システム
開始
W1
文書データ
読み込み
W2
見出し取り出し
または編集
W3
特徴抽出
W4
暗号化
W5
見出しと暗号データ
結合
W6
送信
乙システム
開始
W7
受信
W8
見出しと
暗号データ分離
W9
暗号データと
認証データ結合
W10
暗号化
W11
見出しと
暗号データ結合
W12
送信
終了
外部認証システム
開始
W13
受信
W14
見出しと
暗号データ分離
W15
暗号データと
認証データ結合
W16
暗号化
W17
見出しと
暗号データ結合
W18
送信
終了
W19
受信
W20
文書データと
認証データ結合
終了

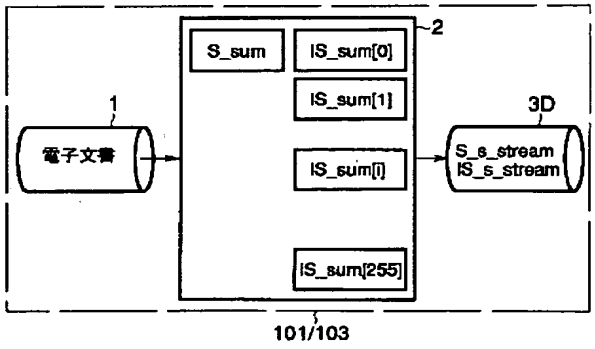
【図１５】



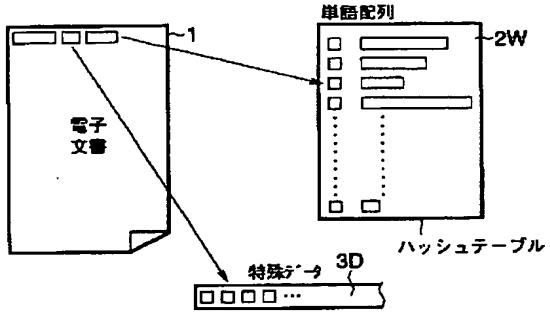
【図１６】



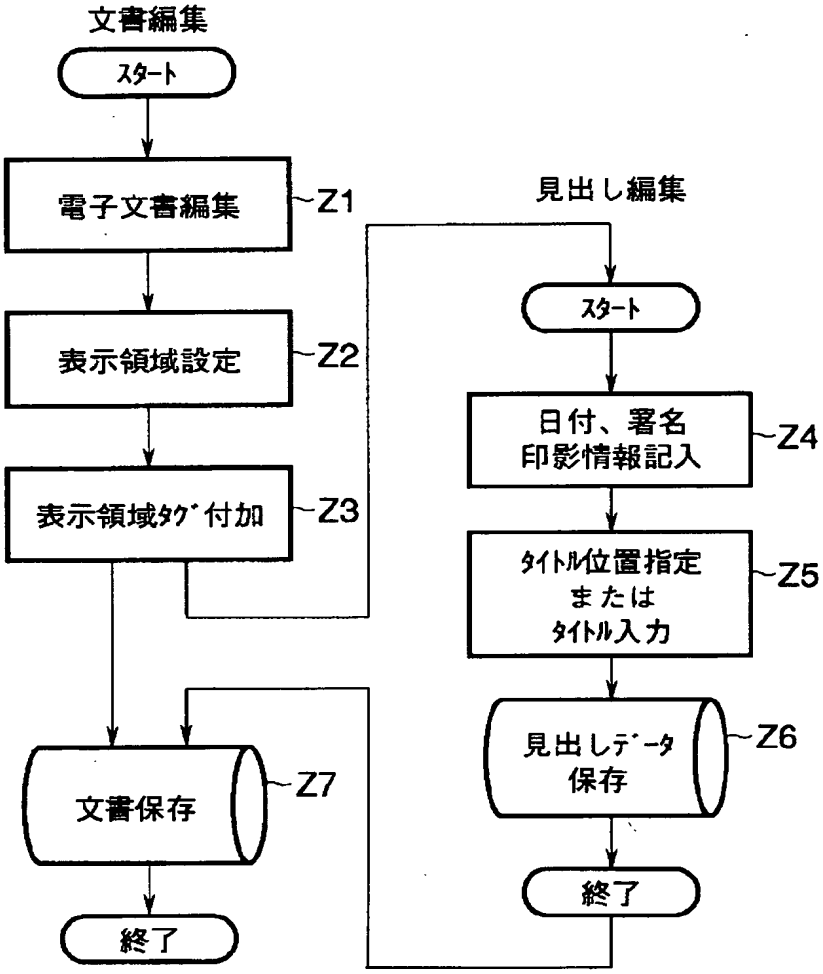
【図２１】



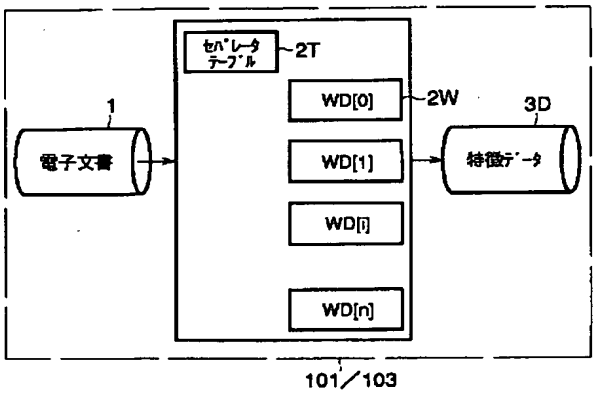
【図２４】



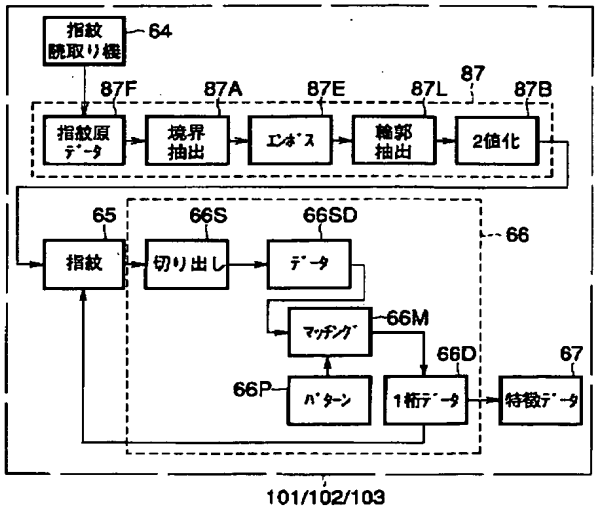
【図１９】


文書編集
スタート
電子文書編集
Z1
表示領域設定
Z2
表示領域ﾀｸﾞ付加
Z3
文書保存
Z7
終了
見出し編集
スタート
日付、署名
印影情報記入
Z4
ﾀｲﾄﾙ位置指定
または
ﾀｲﾄﾙ入力
Z5
見出しﾃﾞｰﾀ
保存
Z6
終了

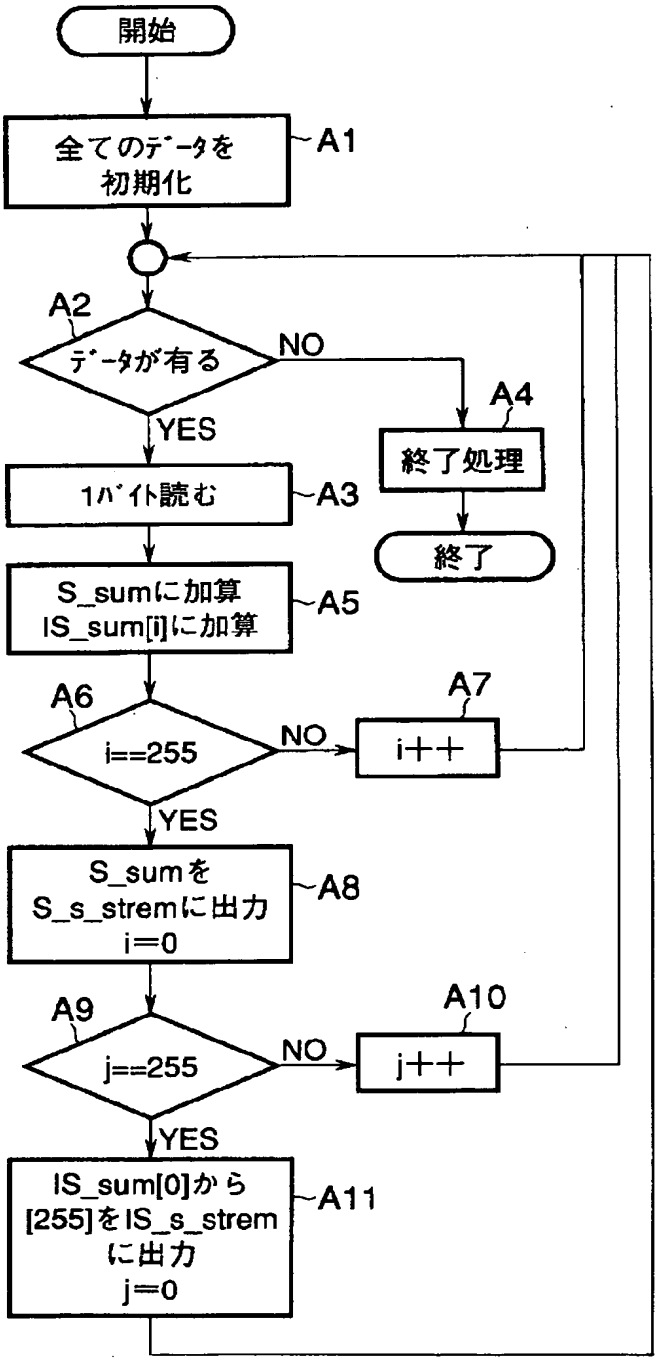
【図２５】


ｾﾊﾟﾚｰﾀ
ﾃｰﾌﾞﾙ
2T
WD[0]
WD[1]
WD[i]
WD[n]
2W
3D
特徴ﾃﾞｰﾀ
1
電子文書
101／103

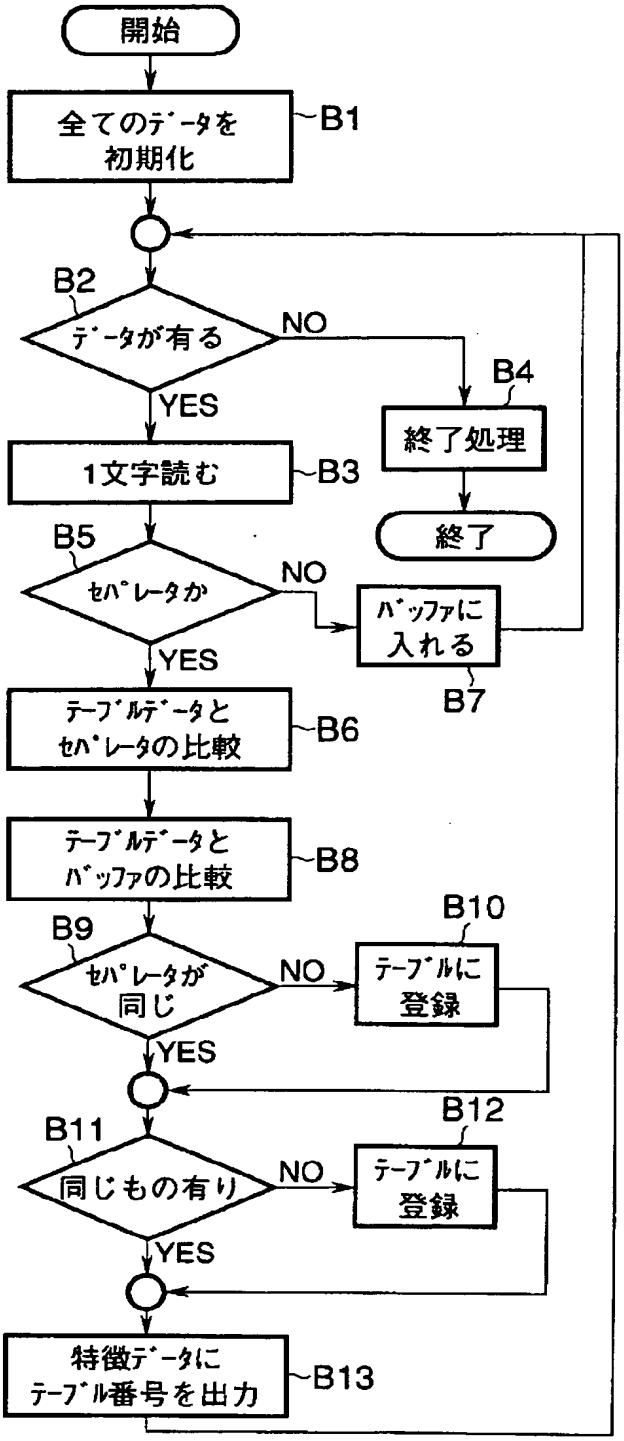
【図３１】


指紋
読取り機
64
87F
87A
87E
87L
87
87B
指紋原
ﾃﾞｰﾀ
境界
抽出
ｴｯｼﾞ
輪郭
抽出
2値化
65
66S
66SD
66
指紋
切り出し
ﾃﾞｰﾀ
ﾏｯﾁﾝｸﾞ
66M
66D
67
66P
ﾊﾟﾀｰﾝ
1桁ﾃﾞｰﾀ
特徴ﾃﾞｰﾀ
101/102/103

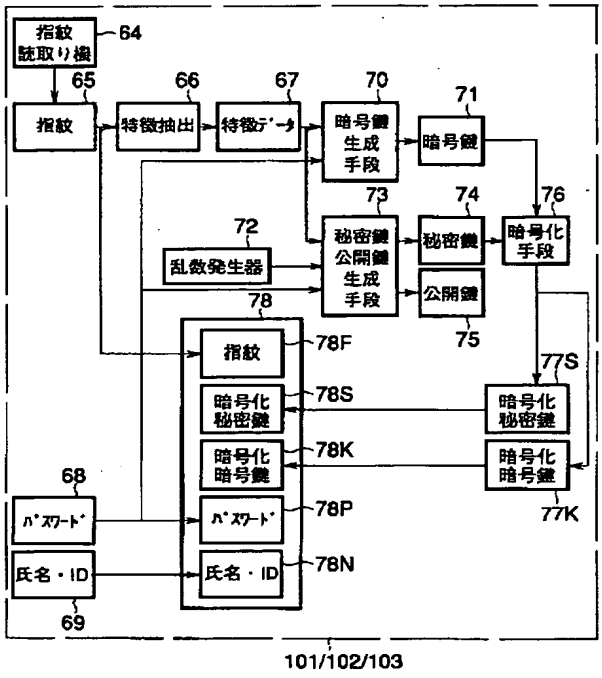
【図２２】


開始
全てのﾃﾞｰﾀを
初期化
A1
A2
ﾃﾞｰﾀが有る
NO
YES
A4
終了処理
終了
1ﾊﾞｲﾄ読む
A3
S_sumに加算
IS_sum[i]に加算
A5
A6
i==255
NO
A7
i++
YES
S_sumを
S_s_stremに出力
i=0
A8
A9
j==255
NO
A10
j++
YES
IS_sum[0]から
[255]をIS_s_strem
に出力
j=0
A11

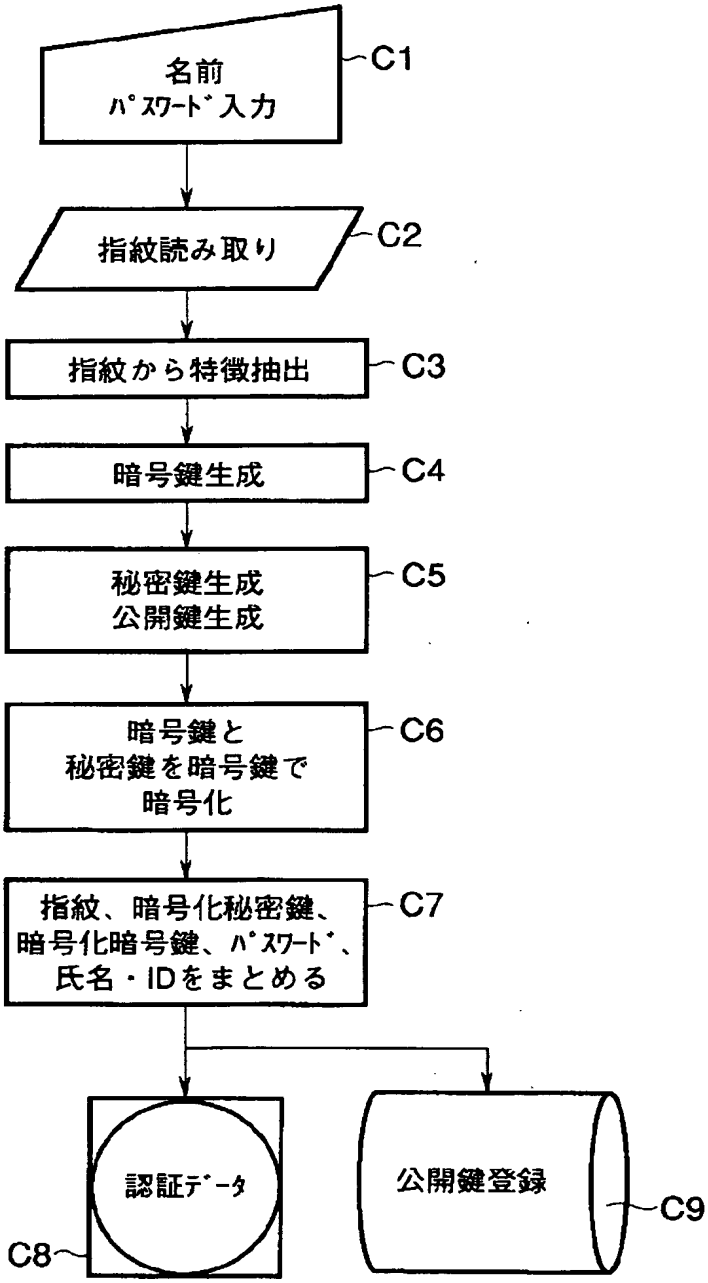
【図２６】


開始
全てのﾃﾞｰﾀを
初期化
B1
B2
ﾃﾞｰﾀが有る
NO
YES
B4
終了処理
終了
1文字読む
B3
B5
ｾﾊﾟﾚｰﾀか
NO
YES
ﾊﾞｯﾌｧに
入れる
B7
ﾃｰﾌﾞﾙﾃﾞｰﾀと
ｾﾊﾟﾚｰﾀの比較
B6
ﾃｰﾌﾞﾙﾃﾞｰﾀと
ﾊﾞｯﾌｧの比較
B8
B9
ｾﾊﾟﾚｰﾀが
同じ
NO
YES
B10
ﾃｰﾌﾞﾙに
登録
B11
同じもの有り
NO
YES
B12
ﾃｰﾌﾞﾙに
登録
特徴ﾃﾞｰﾀに
ﾃｰﾌﾞﾙ番号を出力
B13

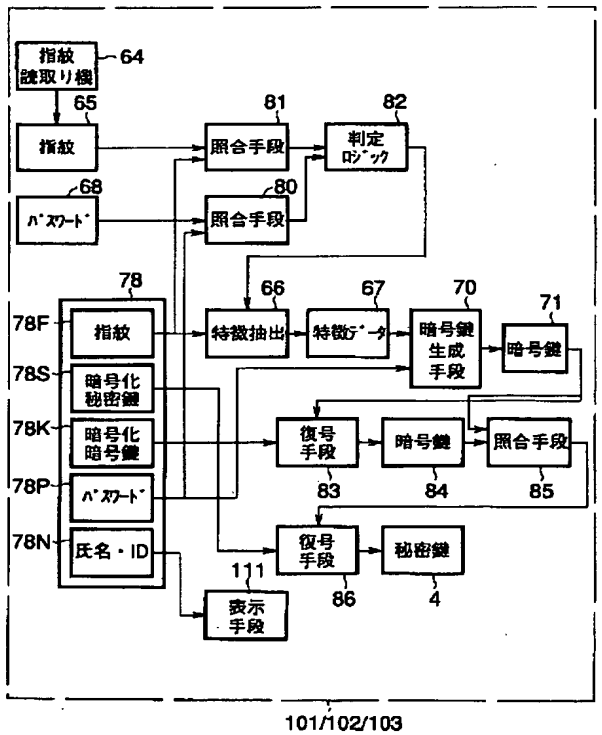
【図２７】


指紋読取り機
64
65
指紋
66
特徴抽出
67
特徴ﾃﾞｰﾀ
70
暗号鍵生成手段
71
暗号鍵
72
乱数発生器
73
秘密鍵公開鍵生成手段
74
秘密鍵
75
公開鍵
76
暗号化手段
77S
78
指紋
78F
暗号化秘密鍵
78S
暗号化暗号鍵
78K
ﾊﾟｽﾜｰﾄﾞ
78P
氏名・ID
78N
68
ﾊﾟｽﾜｰﾄﾞ
氏名・ID
69
77K
101/102/103

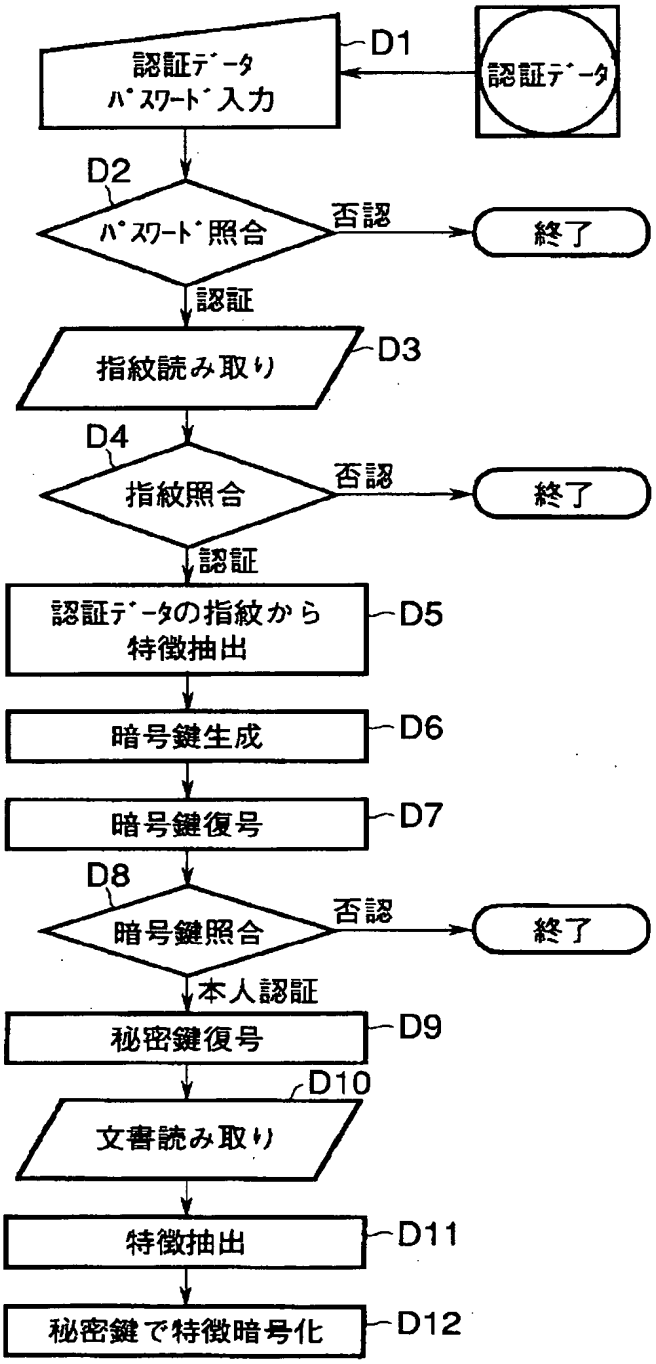
【図２８】


名前
ﾊﾟｽﾜｰﾄﾞ入力
C1
指紋読み取り
C2
指紋から特徴抽出
C3
暗号鍵生成
C4
秘密鍵生成
公開鍵生成
C5
暗号鍵と
秘密鍵を暗号鍵で
暗号化
C6
指紋、暗号化秘密鍵、
暗号化暗号鍵、ﾊﾟｽﾜｰﾄﾞ、
氏名・IDをまとめる
C7
認証ﾃﾞｰﾀ
C8
公開鍵登録
C9

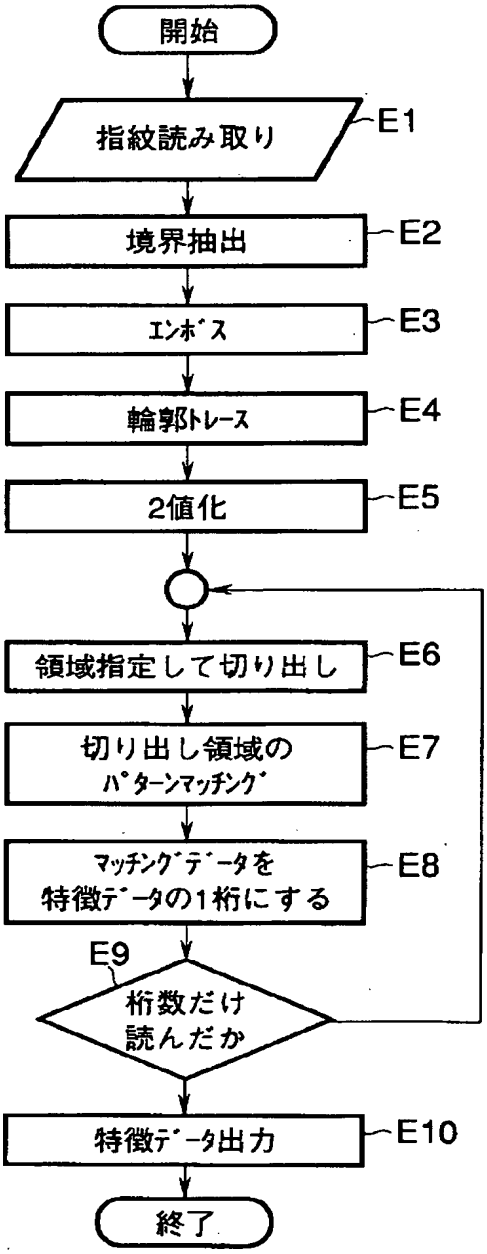
【図２９】


指紋読取り機
64
65
指紋
81
照合手段
82
判定ﾛｼﾞｯｸ
68
ﾊﾟｽﾜｰﾄﾞ
80
照合手段
78
78F
指紋
78S
暗号化秘密鍵
78K
暗号化暗号鍵
78P
ﾊﾟｽﾜｰﾄﾞ
78N
氏名・ID
66
特徴抽出
67
特徴ﾃﾞｰﾀ
70
暗号鍵生成手段
71
暗号鍵
復号手段
83
暗号鍵
84
照合手段
85
復号手段
86
秘密鍵
4
111
表示手段
101/102/103

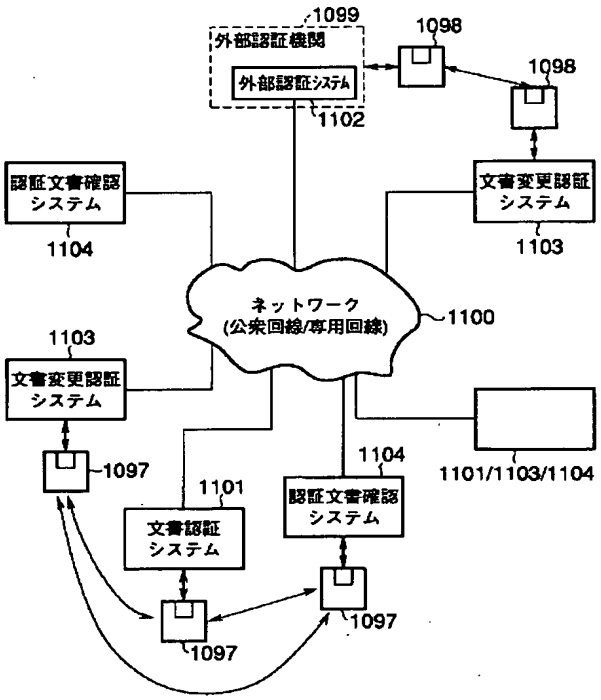
【図３０】


認証ﾃﾞｰﾀ
ﾊﾟｽﾜｰﾄﾞ入力
D1
認証ﾃﾞｰﾀ
D2
ﾊﾟｽﾜｰﾄﾞ照合
否認
終了
認証
指紋読み取り
D3
D4
指紋照合
否認
終了
認証
認証ﾃﾞｰﾀの指紋から
特徴抽出
D5
暗号鍵生成
D6
暗号鍵復号
D7
D8
暗号鍵照合
否認
終了
本人認証
秘密鍵復号
D9
D10
文書読み取り
特徴抽出
D11
秘密鍵で特徴暗号化
D12

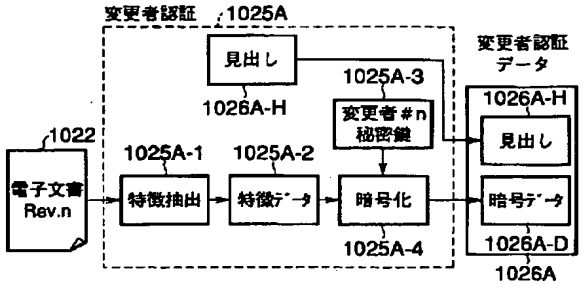
【図３５】


開始
指紋読み取り
E1
境界抽出
E2
ｴﾝﾎﾞｽ
E3
輪郭ﾄﾚｰｽ
E4
2値化
E5
領域指定して切り出し
E6
切り出し領域の
ﾊﾟﾀｰﾝﾏｯﾁﾝｸﾞ
E7
ﾏｯﾁﾝｸﾞﾃﾞｰﾀを
特徴ﾃﾞｰﾀの1桁にする
E8
E9
桁数だけ
読んだか
特徴ﾃﾞｰﾀ出力
E10
終了

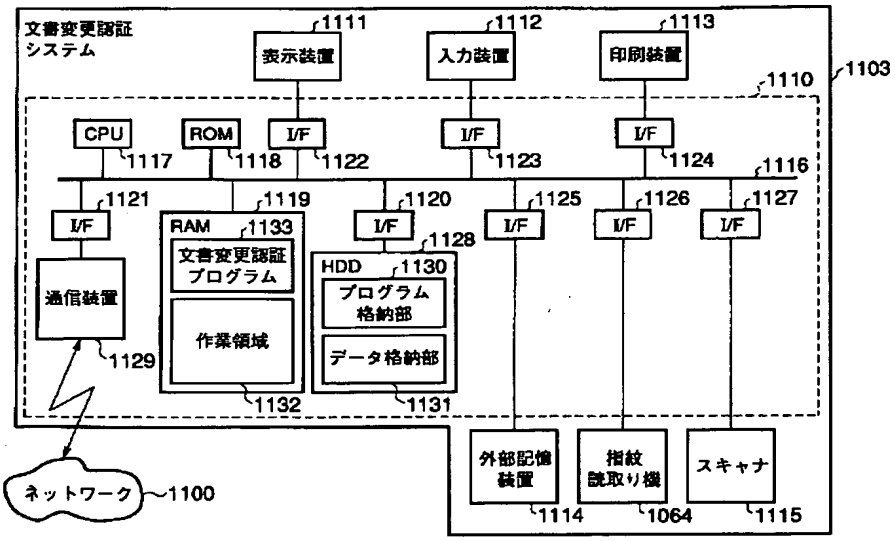
【図３６】


外部認証機関
外部認証システム
1099
1098
1098
1102
認証文書確認システム
1104
文書変更認証システム
1103
ネットワーク
(公衆回線/専用回線)
1100
1103
文書変更認証システム
1097
1101
文書認証システム
1104
認証文書確認システム
1101/1103/1104
1097
1097

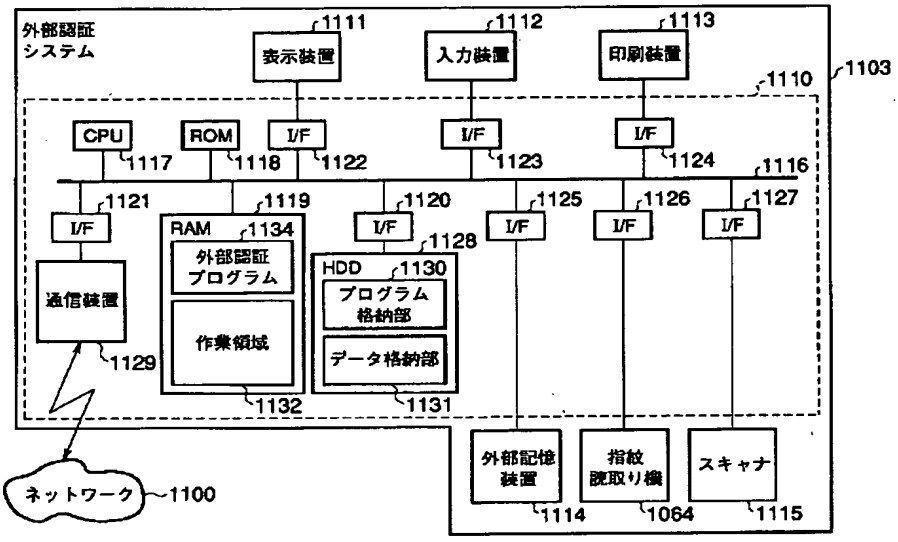
【図４１】


変更者認証
1025A
見出し
1026A-H
1025A-3
変更者#n秘密鍵
1022
電子文書 Rev.n
1025A-1
特徴抽出
1025A-2
特徴データ
暗号化
1025A-4
変更者認証データ
1026A-H
見出し
暗号データ
1026A-D
1026A

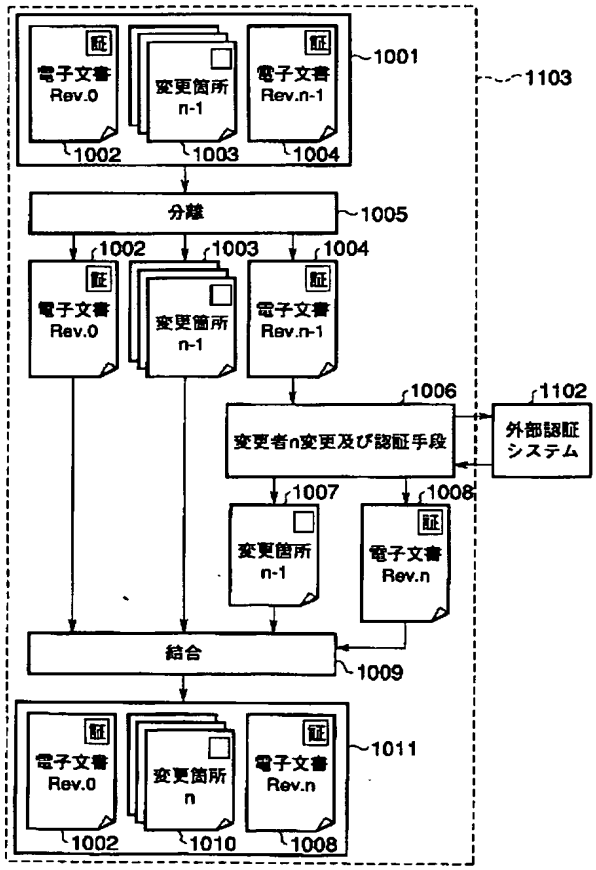
【図３７】


文書変更認証システム
1111
表示装置
1112
入力装置
1113
印刷装置
1110
1103
CPU
1117
ROM
1118
I/F
1122
I/F
1123
I/F
1124
1116
I/F
1121
RAM
1133
1119
文書変更認証プログラム
作業領域
1132
I/F
1120
HDD
1130
1128
プログラム格納部
データ格納部
1131
I/F
1125
I/F
1126
I/F
1127
通信装置
1129
ネットワーク
1100
外部記憶装置
1114
指紋読取り機
1064
スキャナ
1115

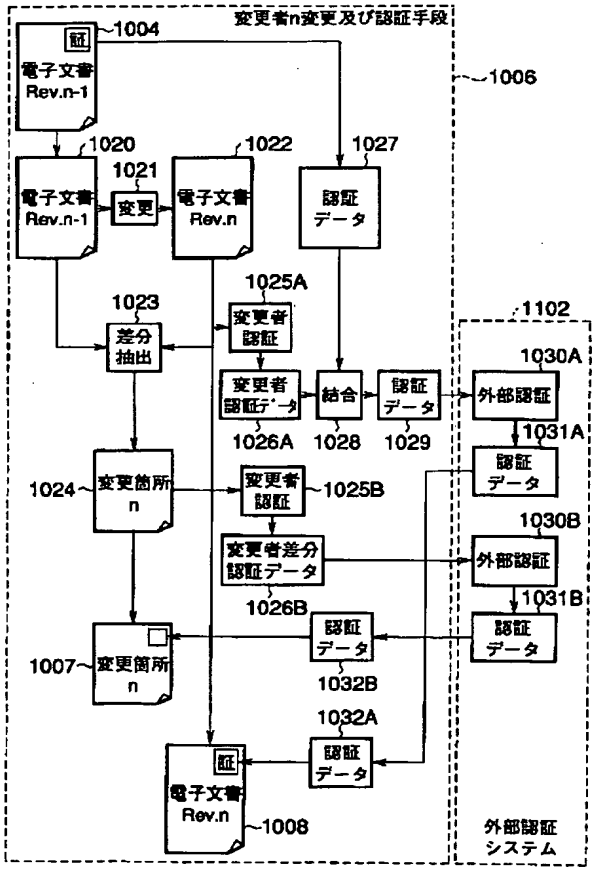
【図３８】


外部認証
システム
表示装置
1111
入力装置
1112
印刷装置
1113
1110
1103
CPU
1117
ROM
1118
I/F
1122
I/F
1123
I/F
1124
1116
I/F
1121
RAM
1134
外部認証
プログラム
作業領域
1119
I/F
1120
HDD
1130
プログラム
格納部
データ格納部
1128
I/F
1125
I/F
1126
I/F
1127
通信装置
1129
1132
1131
外部記憶
装置
1114
指紋
読取り機
1064
スキャナ
1115
ネットワーク
1100

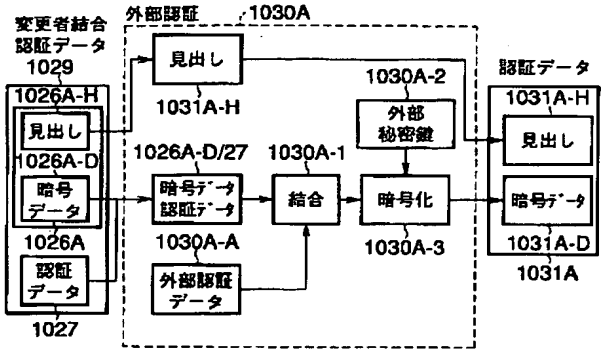
【図３９】


証
電子文書
Rev.0
1002
変更箇所
n-1
1003
電子文書
Rev.n-1
1004
1001
1103
分離
1005
1002
1003
1004
電子文書
Rev.0
変更箇所
n-1
電子文書
Rev.n-1
1006
変更者n変更及び認証手段
1102
外部認証
システム
1007
変更箇所
n-1
1008
電子文書
Rev.n
結合
1009
電子文書
Rev.0
1002
変更箇所
n
1010
電子文書
Rev.n
1008
1011

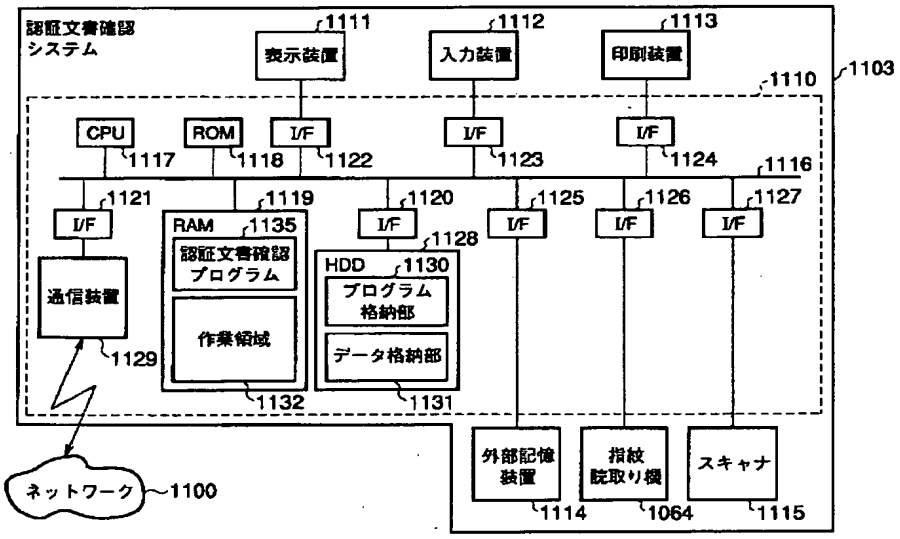
【図４０】


変更者n変更及び認証手段
1004
電子文書
Rev.n-1
1006
1020
電子文書
Rev.n-1
1021
変更
1022
電子文書
Rev.n
1027
認証
データ
1025A
1023
差分
抽出
変更者
認証
1102
1030A
外部認証
1031A
認証
データ
変更者
認証データ
1026A
結合
1028
認証
データ
1029
1024
変更箇所
n
変更者
認証
1025B
1030B
外部認証
1031B
認証
データ
変更者差分
認証データ
1026B
1007
変更箇所
n
認証
データ
1032B
1032A
認証
データ
証
電子文書
Rev.n
1008
外部認証
システム

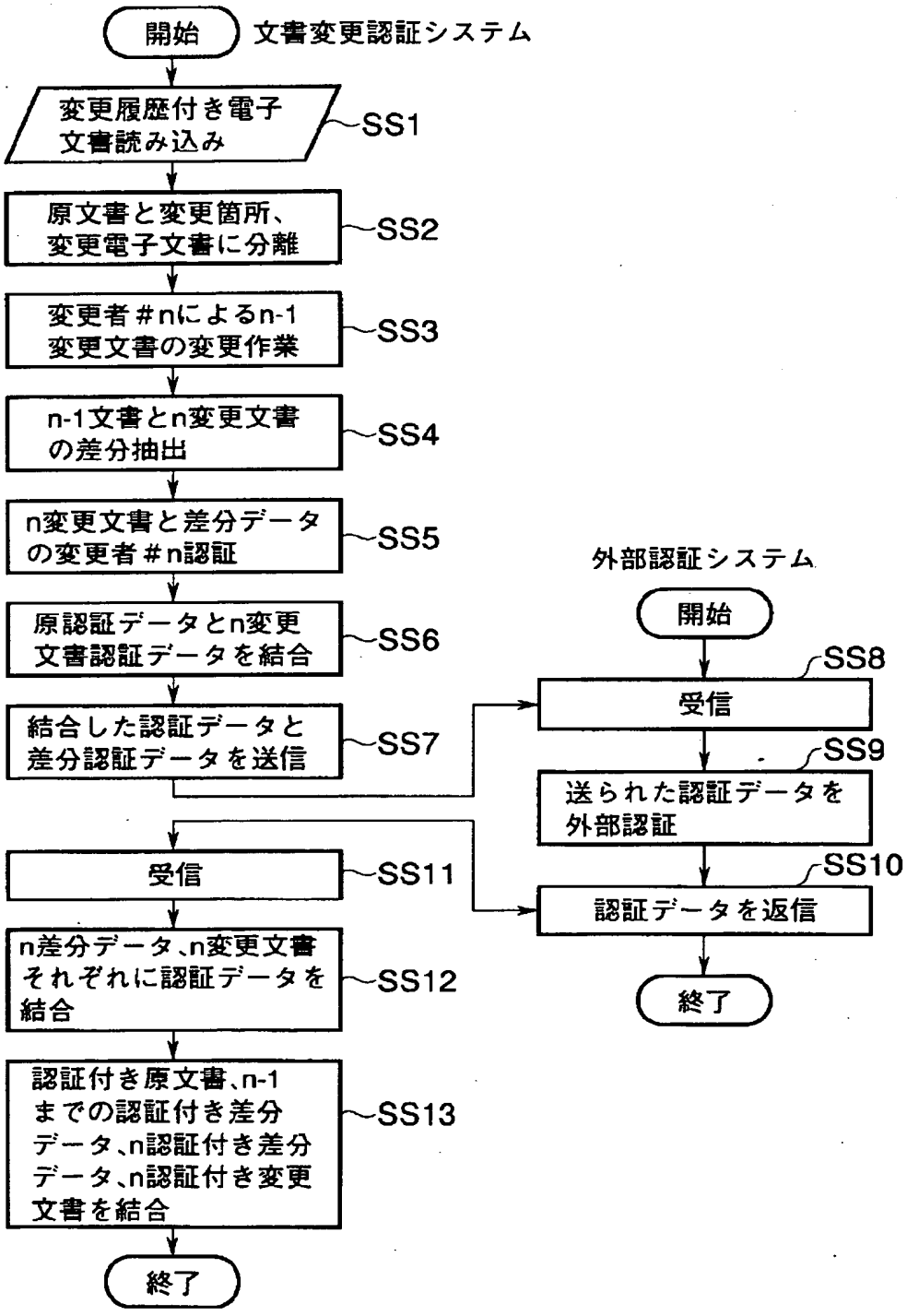
【図４２】


変更者結合
認証データ
1029
1026A-H
見出し
1026A-D
暗号
データ
1026A
認証
データ
1027
外部認証
1030A
見出し
1031A-H
1026A-D/27
暗号ﾃﾞｰﾀ
認証ﾃﾞｰﾀ
1030A-A
外部認証
データ
1030A-1
結合
1030A-2
外部
秘密鍵
暗号化
1030A-3
認証データ
1031A-H
見出し
暗号ﾃﾞｰﾀ
1031A-D
1031A

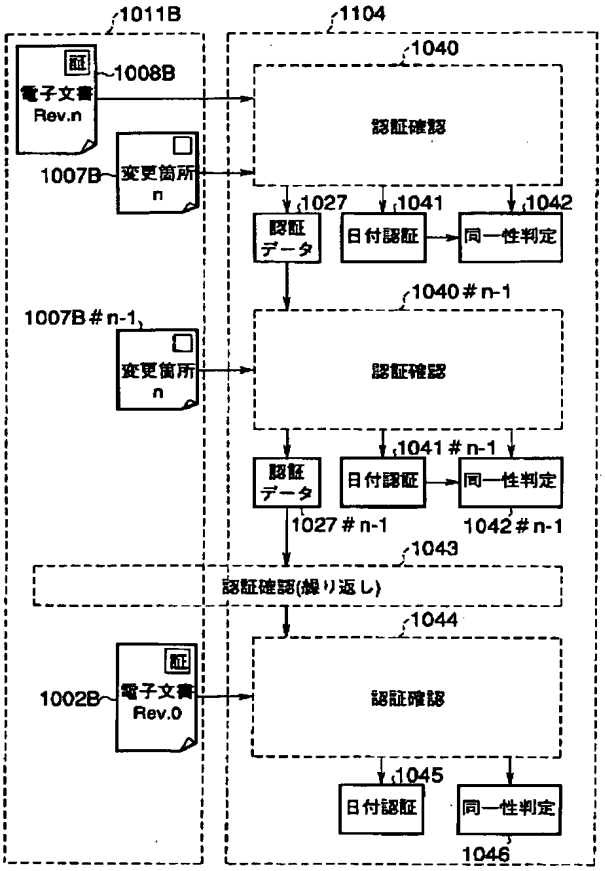
【図４４】


認証文書確認
システム
1111
表示装置
1112
入力装置
1113
印刷装置
1110
1103
CPU
1117
ROM
1118
I/F
1122
I/F
1123
I/F
1124
1116
1121
I/F
通信装置
1129
RAM
1135
認証文書確認
プログラム
作業領域
1132
1119
1120
I/F
1128
HDD
1130
プログラム
格納部
データ格納部
1131
1125
I/F
1126
I/F
1127
I/F
ネットワーク
1100
外部記憶
装置
1114
指紋
読取り機
1064
スキャナ
1115

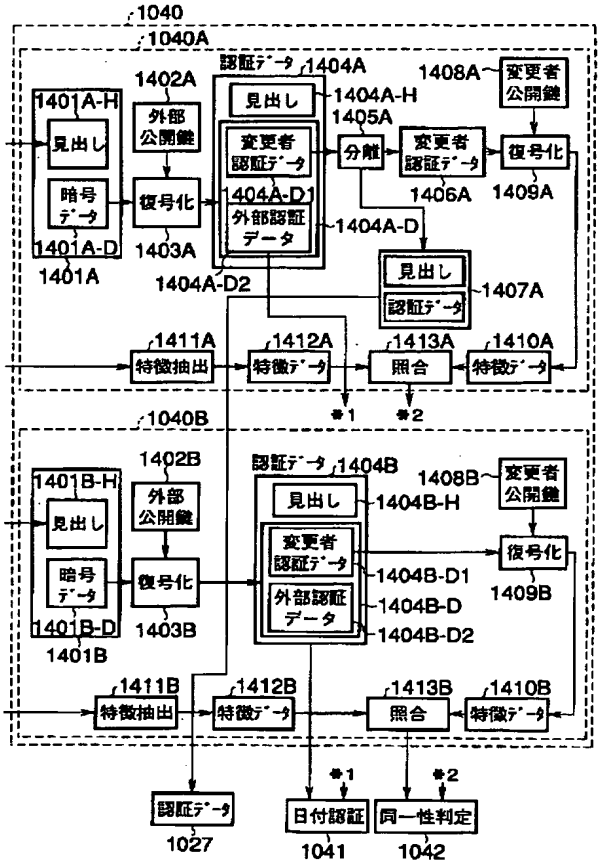
【図４３】


開始
文書変更認証システム
変更履歴付き電子文書読み込み
SS1
原文書と変更箇所、変更電子文書に分離
SS2
変更者＃nによるn-1変更文書の変更作業
SS3
n-1文書とn変更文書の差分抽出
SS4
n変更文書と差分データの変更者＃n認証
SS5
原認証データとn変更文書認証データを結合
SS6
結合した認証データと差分認証データを送信
SS7
外部認証システム
開始
受信
SS8
送られた認証データを外部認証
SS9
認証データを返信
SS10
終了
受信
SS11
n差分データ、n変更文書それぞれに認証データを結合
SS12
認証付き原文書、n-1までの認証付き差分データ、n認証付き差分データ、n認証付き変更文書を結合
SS13
終了

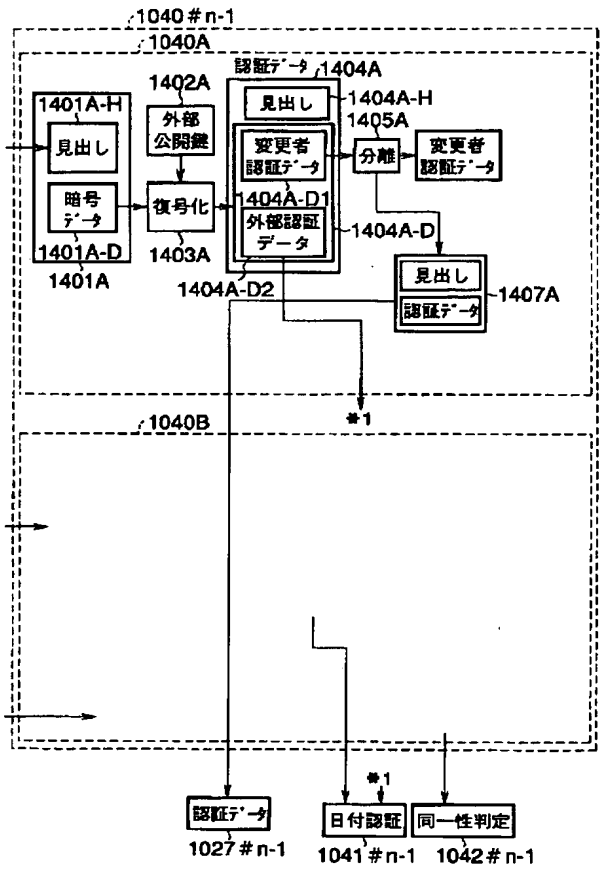
【図４５】


1011B
1104
1040
証
1008B
電子文書
Rev.n
認証確認
1007B
変更箇所
n
1027
1041
1042
認証
データ
日付認証
同一性判定
1040＃n-1
1007B＃n-1
変更箇所
n
認証確認
1041＃n-1
認証
データ
日付認証
同一性判定
1027＃n-1
1042＃n-1
1043
認証確認(繰り返し)
1044
証
1002B
電子文書
Rev.0
認証確認
1045
日付認証
同一性判定
1046

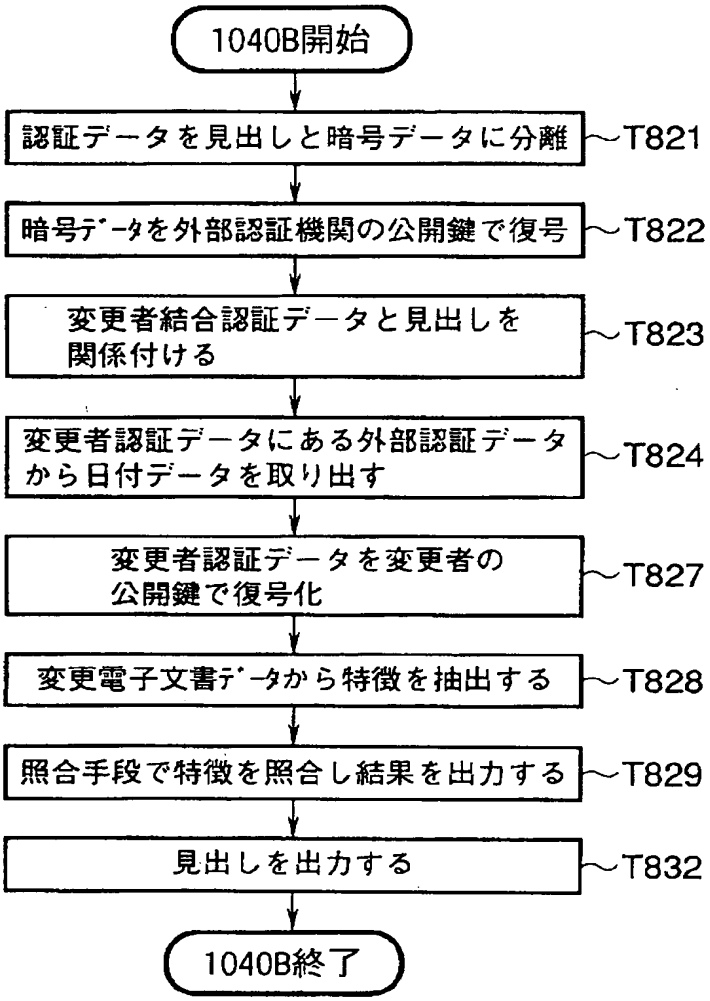
【図４６】


1040
1040A
認証ﾃﾞｰﾀ
1404A
1408A
変更者
公開鍵
1402A
外部
公開鍵
見出し
1404A-H
1401A-H
見出し
1405A
変更者
認証ﾃﾞｰﾀ
分離
変更者
認証ﾃﾞｰﾀ
復号化
1409A
1406A
暗号
ﾃﾞｰﾀ
復号化
1404A-D1
外部認証
データ
1404A-D
1401A-D
1401A
1403A
1404A-D2
見出し
認証ﾃﾞｰﾀ
1407A
1411A
1412A
1413A
1410A
特徴抽出
特徴ﾃﾞｰﾀ
照合
特徴ﾃﾞｰﾀ
＊1
＊2
1040B
1402B
認証ﾃﾞｰﾀ
1404B
1408B
変更者
公開鍵
1401B-H
外部
公開鍵
見出し
1404B-H
見出し
変更者
認証ﾃﾞｰﾀ
復号化
1404B-D1
1409B
暗号
ﾃﾞｰﾀ
復号化
外部認証
データ
1404B-D
1404B-D2
1401B-D
1401B
1403B
1411B
1412B
1413B
1410B
特徴抽出
特徴ﾃﾞｰﾀ
照合
特徴ﾃﾞｰﾀ
＊1
＊2
認証ﾃﾞｰﾀ
日付認証
同一性判定
1027
1041
1042

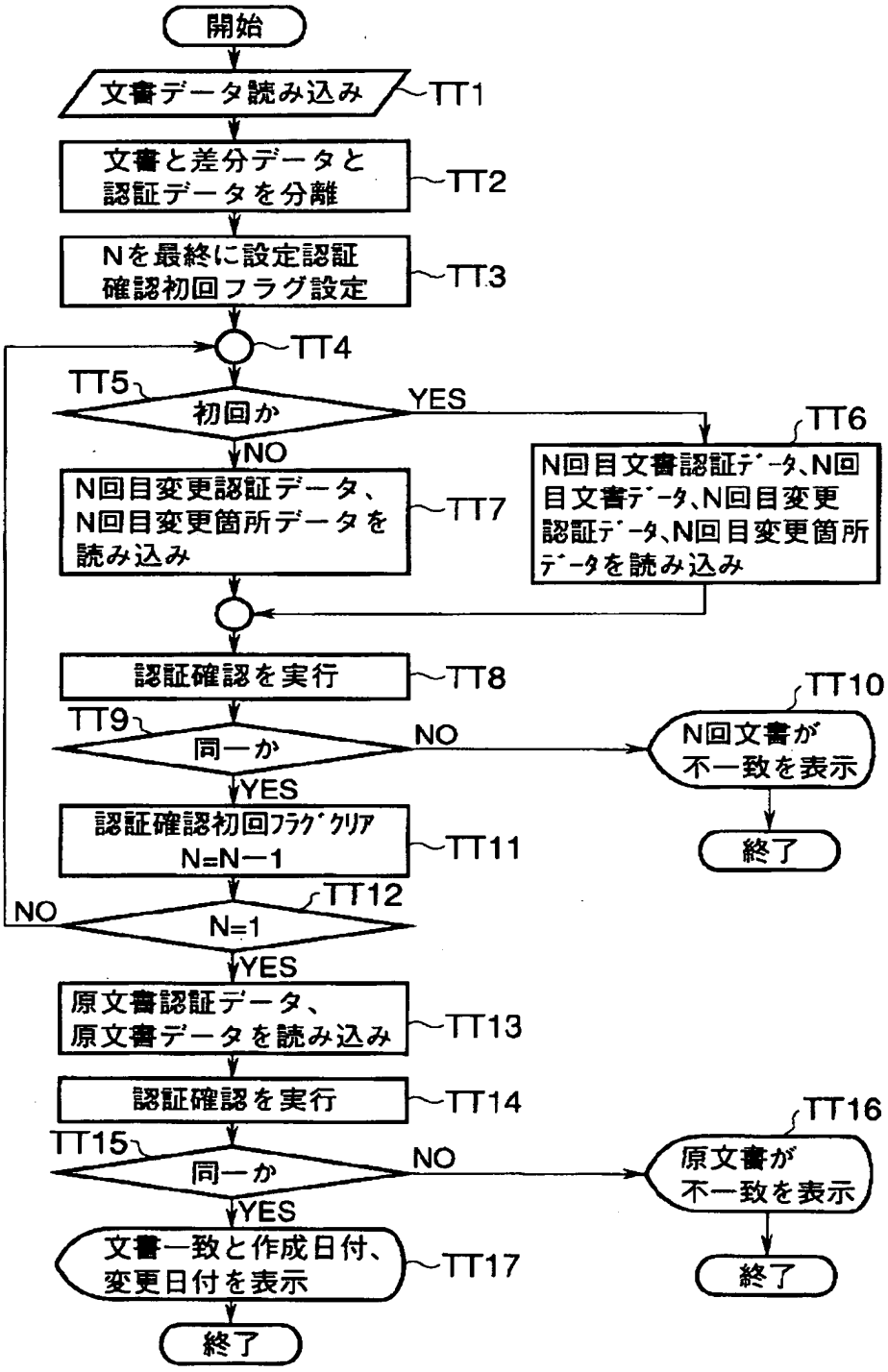
【図４７】


1040＃n-1
1040A
認証ﾃﾞｰﾀ
1404A
1402A
1401A-H
見出し
外部公開鍵
1404A-H
1405A
分離
変更者認証ﾃﾞｰﾀ
変更者認証ﾃﾞｰﾀ
暗号ﾃﾞｰﾀ
復号化
404A-D1
外部認証データ
1404A-D
1401A-D
1403A
1401A
1404A-D2
見出し
認証ﾃﾞｰﾀ
1407A
＊1
1040B
＊1
認証ﾃﾞｰﾀ
日付認証
同一性判定
1027＃n-1
1041＃n-1
1042＃n-1

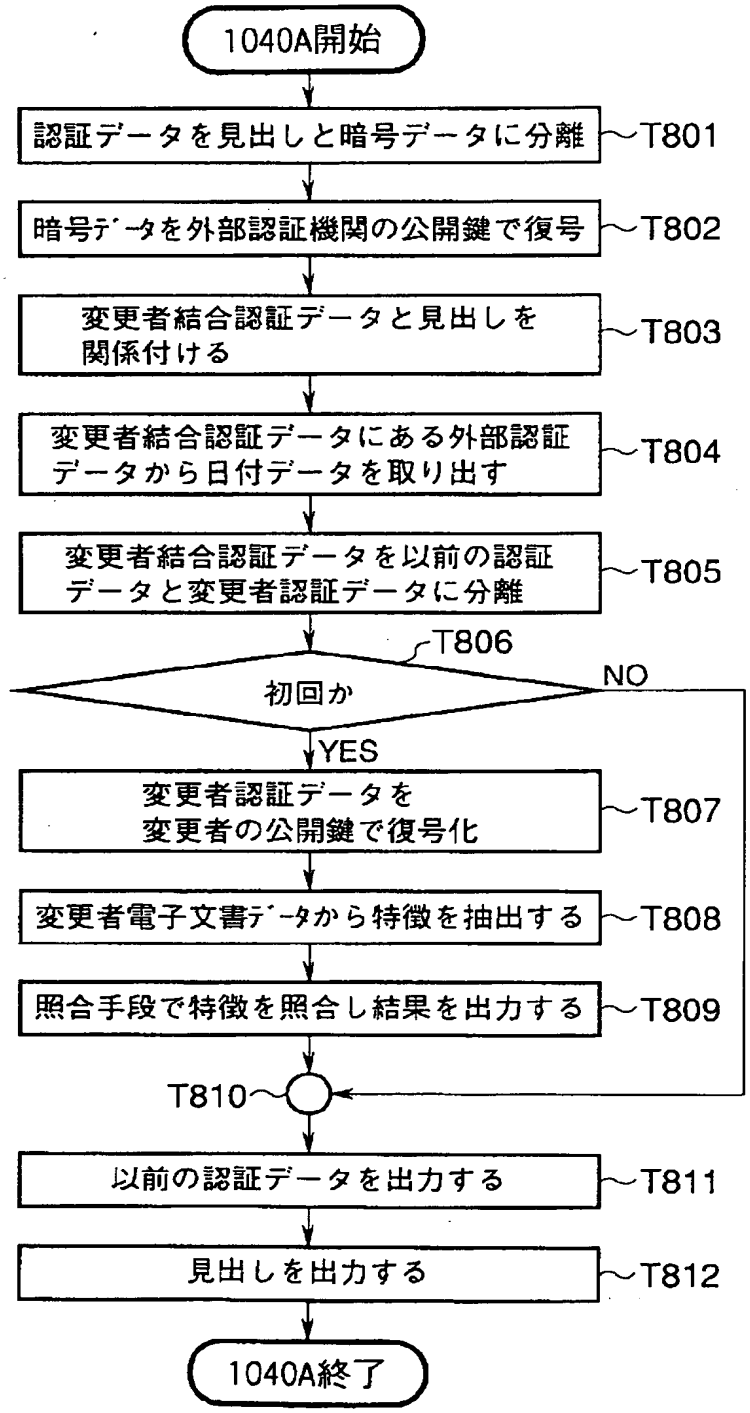
【図５０】


1040B開始
認証データを見出しと暗号データに分離
T821
暗号ﾃﾞｰﾀを外部認証機関の公開鍵で復号
T822
変更者結合認証データと見出しを関係付ける
T823
変更者認証データにある外部認証データから日付データを取り出す
T824
変更者認証データを変更者の公開鍵で復号化
T827
変更電子文書ﾃﾞｰﾀから特徴を抽出する
T828
照合手段で特徴を照合し結果を出力する
T829
見出しを出力する
T832
1040B終了

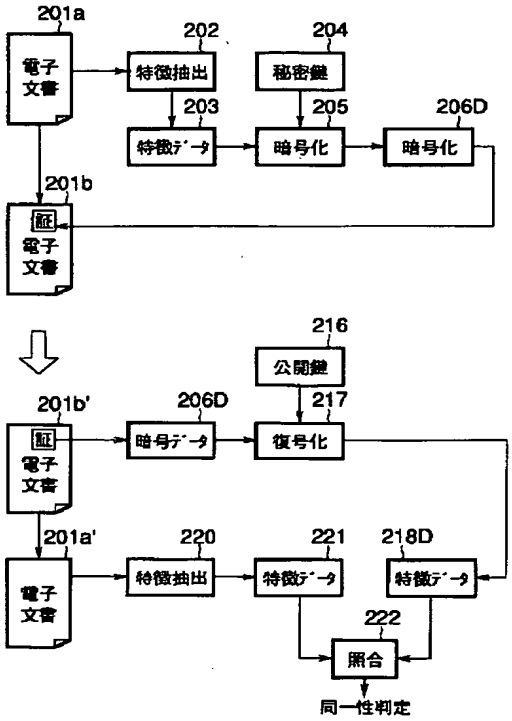
【図４８】


開始
文書データ読み込み
TT1
文書と差分データと認証データを分離
TT2
Nを最終に設定認証確認初回フラグ設定
TT3
TT4
TT5
初回か
YES
TT6
NO
N回目変更認証データ、N回目変更箇所データを読み込み
TT7
N回目文書認証ﾃﾞｰﾀ、N回目文書ﾃﾞｰﾀ、N回目変更認証ﾃﾞｰﾀ、N回目変更箇所ﾃﾞｰﾀを読み込み
認証確認を実行
TT8
TT10
TT9
同一か
NO
N回文書が不一致を表示
YES
終了
認証確認初回ﾌﾗｸﾞｸﾘｱ N=N−1
TT11
TT12
NO
N=1
YES
原文書認証データ、原文書データを読み込み
TT13
認証確認を実行
TT14
TT16
TT15
同一か
NO
原文書が不一致を表示
YES
文書一致と作成日付、変更日付を表示
TT17
終了
終了

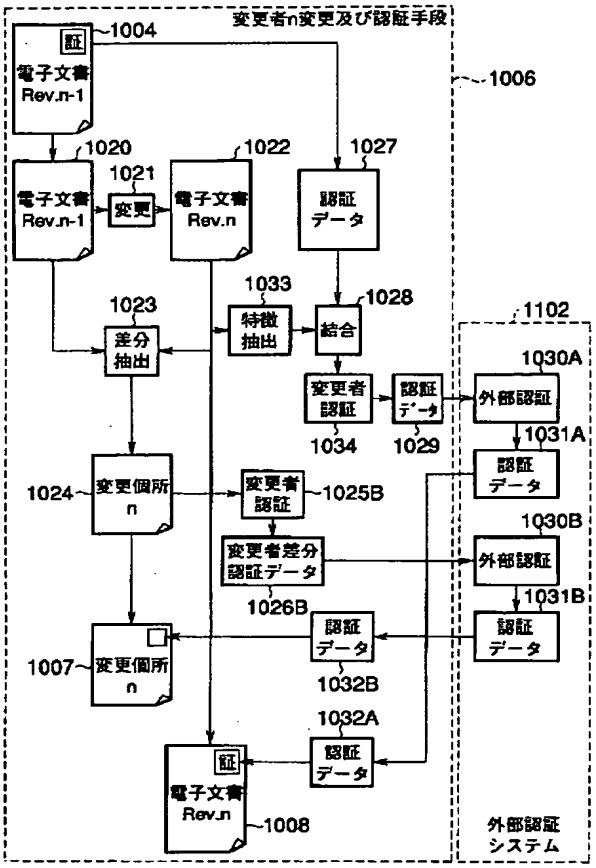
【図４９】


1040A開始
認証データを見出しと暗号データに分離
T801
暗号データを外部認証機関の公開鍵で復号
T802
変更者結合認証データと見出しを関係付ける
T803
変更者結合認証データにある外部認証データから日付データを取り出す
T804
変更者結合認証データを以前の認証データと変更者認証データに分離
T805
T806
初回か
NO
YES
変更者認証データを変更者の公開鍵で復号化
T807
変更者電子文書データから特徴を抽出する
T808
照合手段で特徴を照合し結果を出力する
T809
T810
以前の認証データを出力する
T811
見出しを出力する
T812
1040A終了

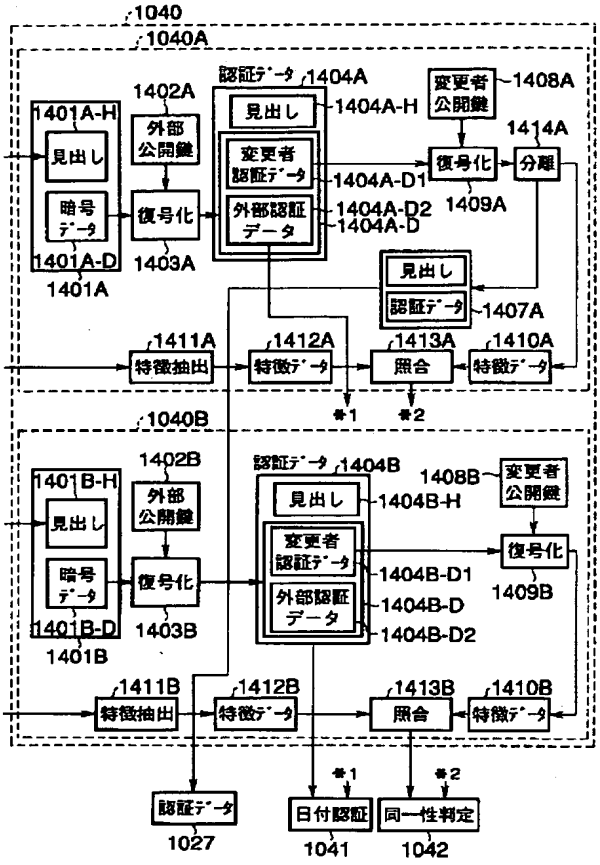
【図５３】


201a
電子文書
202
特徴抽出
204
秘密鍵
203
特徴データ
205
暗号化
206D
暗号化
201b
証
電子文書
216
公開鍵
201b'
206D
217
証
電子文書
暗号データ
復号化
201a'
220
221
218D
電子文書
特徴抽出
特徴データ
特徴データ
222
照合
同一性判定

【図５１】



【図５２】



フロントページの続き

(51) Int. Cl.[6]	識別記号	F I
		H04L 9/00 675D

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☑ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.